

\$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  Wed 6 Feb, 8:55 AM 7 °C 

Feedhunter Rini - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.feedhunter.com/en/  satellite feed hunter dx 

Google  satellite feed hunter dx  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

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
 Sat-Benelux	BVD-sat
Sat4fun	Worldwide webcam and Webcam TV
Sat4All	All digital sat-receivers
Satfeeds.eu	Online Satellite Calculations
Feed Hunters Place	Digi-television
Chitchat	Prog DVB
Sportfeeds	DVB-Dream
Satellite Tracker (info uitzendsatellieten)	Flysat
Feedhuntplaza	Lyngsat
Screenshots Feedhuntplaza	King of Sat
Satboard.nl	Satelliet-link-pagina
Feedhuntplaza	Satlinks-plaza
DXTV.de	Football and other Sport on the Sat. 1
DX-tv	Football and other Sport on the Sat. 2
King of Sat	Football and other Sport on the Sat. 3
Feed-Frequency	Football and other Sport on the Sat. 4
SatBox4All	Football Live. 5
	Free football on Sat 6

Done  Tor Disabled

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

Poking in the dark

Applications Places System Wed 6 Feb, 9:59 AM 7 °C

Feedhuntplaza Satellite Tracker - Mozilla Firefox

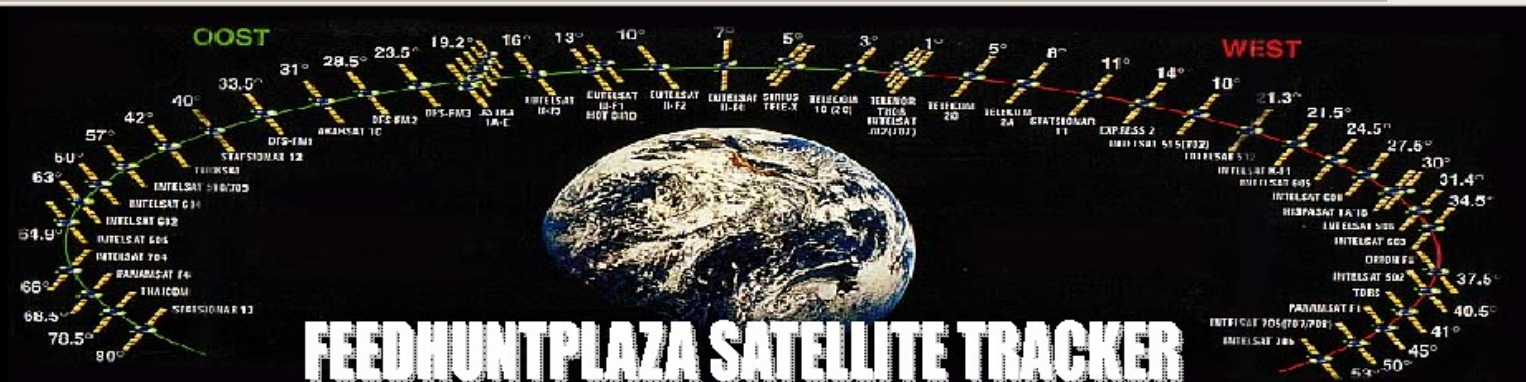
File Edit View History Bookmarks Tools Help

http://www.satplaza.com/orbit/eutelsatw2.html

satellite feed hunter dx

Google satellite feed hunter dx 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 Feedhuntplaza Satellite ...



FEEDHUNTPLAZA SATELLITE TRACKER

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 3F2.

NEDERLANDS

FOOTPRINTS



Click on the picture to enlarge it



Click on the pictures to enlarge it

Done

Feedhuntplaza Satell... screenshots - File Br... Starting Take Screen...

Tor Disabled

Poking in the dark

Applications Places System Wed 6 Feb, 9:00 AM 7 °C

» E 33 Eurobird 3 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.satplaza.com/feedhuntplaza/index.php?cat=6 satellite feed hunter dx

Google satellite feed hunter dx 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 » E 33 Eurobird 3

Feedhuntplaza

SATELLITE TRACKER

ALL INFORMATION ABOUT THE SATELLITES POWERED BY FEEDHUNTPLAZA

JULY 26TH, 2006

TV Spelletje

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 »

Links

- Homepage
- Feedhunt Links
- Satellite Links
- Feed Screenshots
- Satellite Tracker
- Downloads
- Feedhunt Info
- Satplaza Weblog
- Email
- Registration

Screenshots

- 07 East Feeds
- 10 East Feeds
- 16 East Feeds
- HOL 172 Feeds
- Laakerkwartier
- NOS Olympics
- Olympics 2004
- Testcards

Login/Register

Login

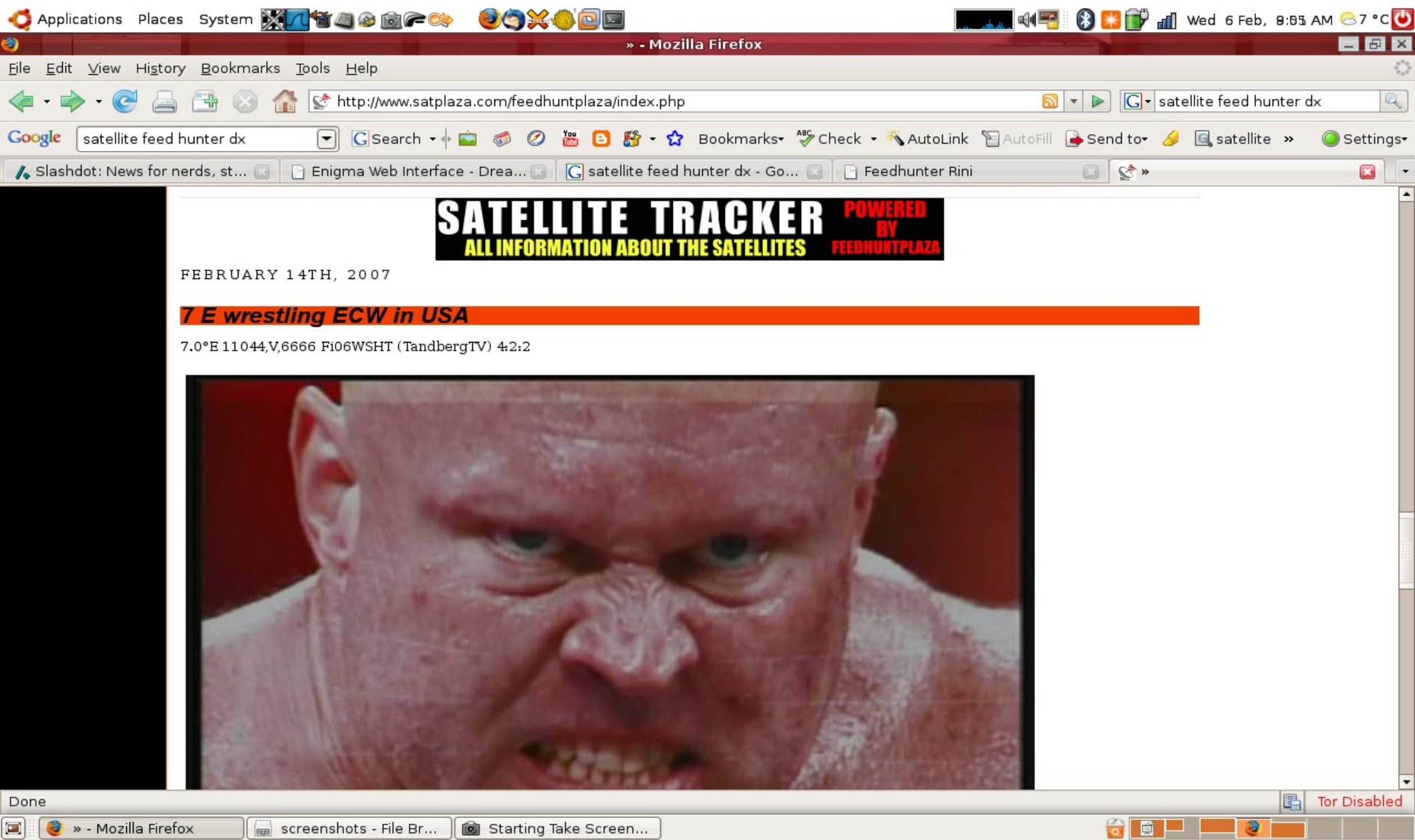
Satellites

- Algmeen / 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

Done Tor Disabled

» E 33 Eurobird 3 - M... Starting Take Screen...

Poking in the dark

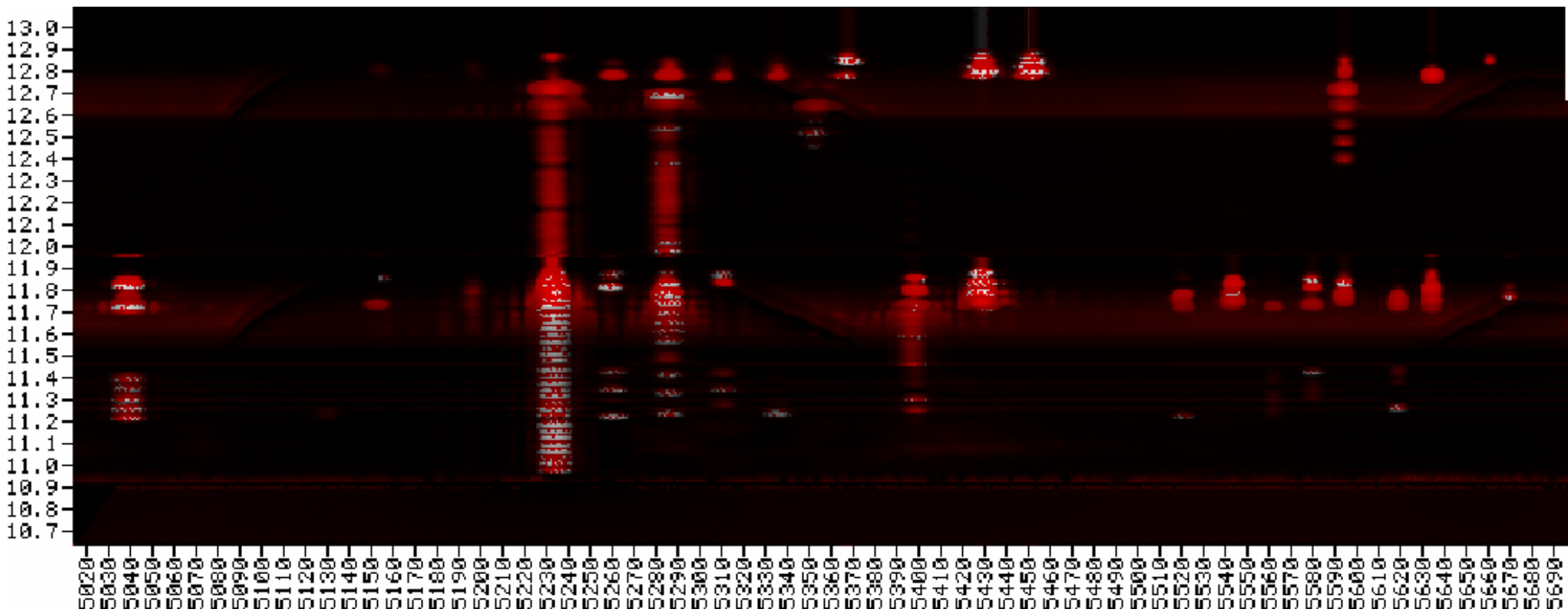


There must be a better way!

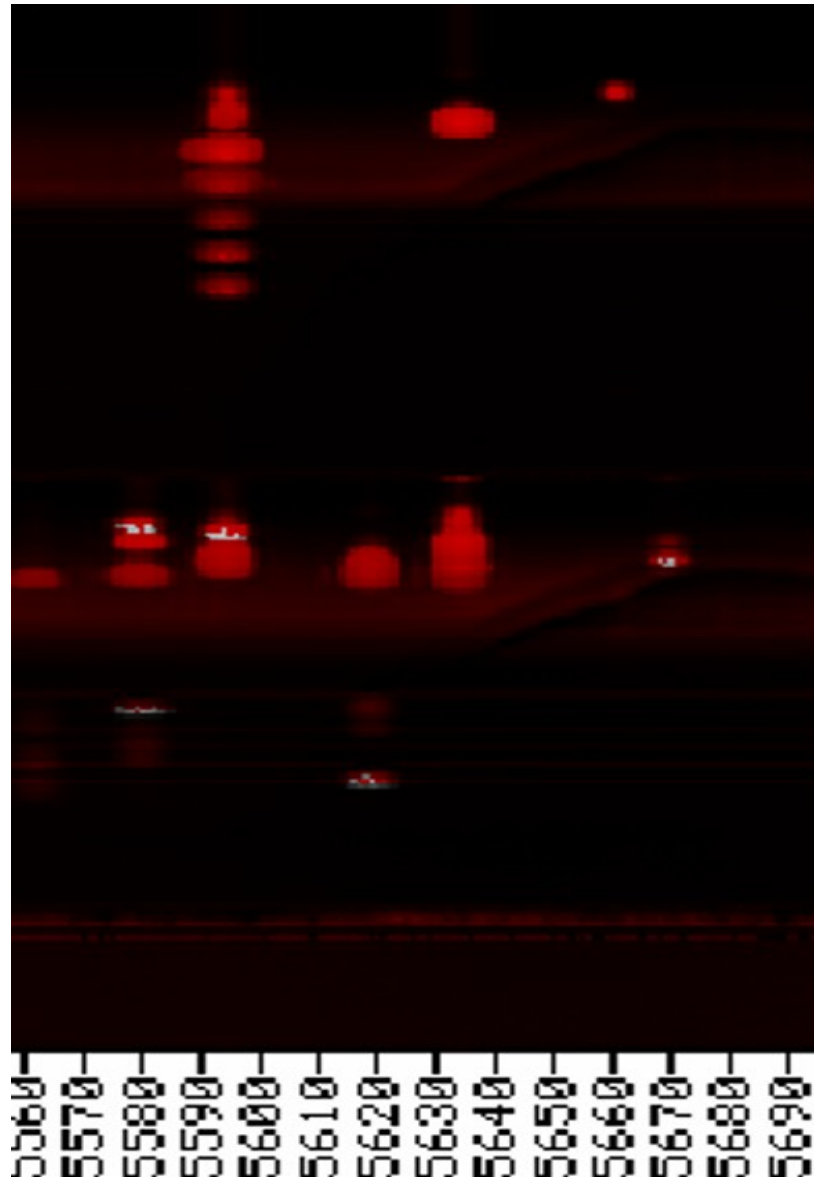
- Visualisation is your friend
 - Human Brain likes images
 - Recognise food
 - Recognise danger
 - Recognise friends
 - Recognise enemies

Visual Representations

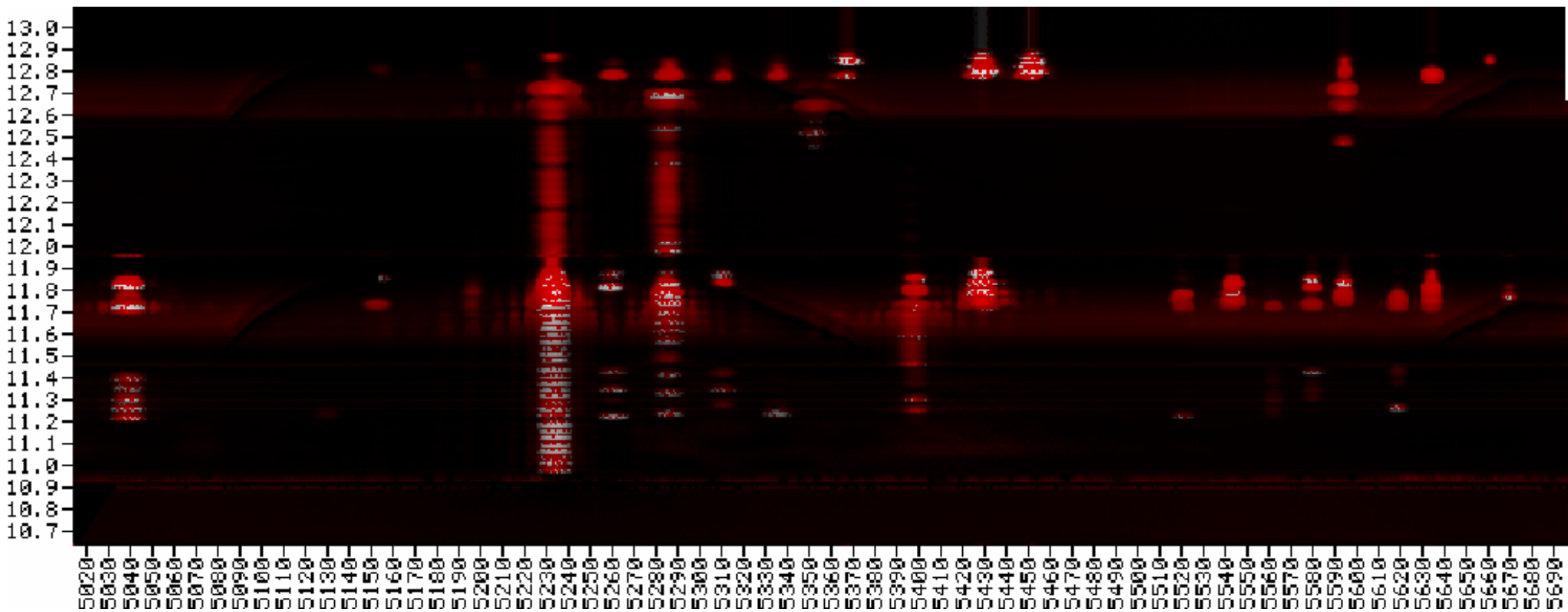
Visual Representations



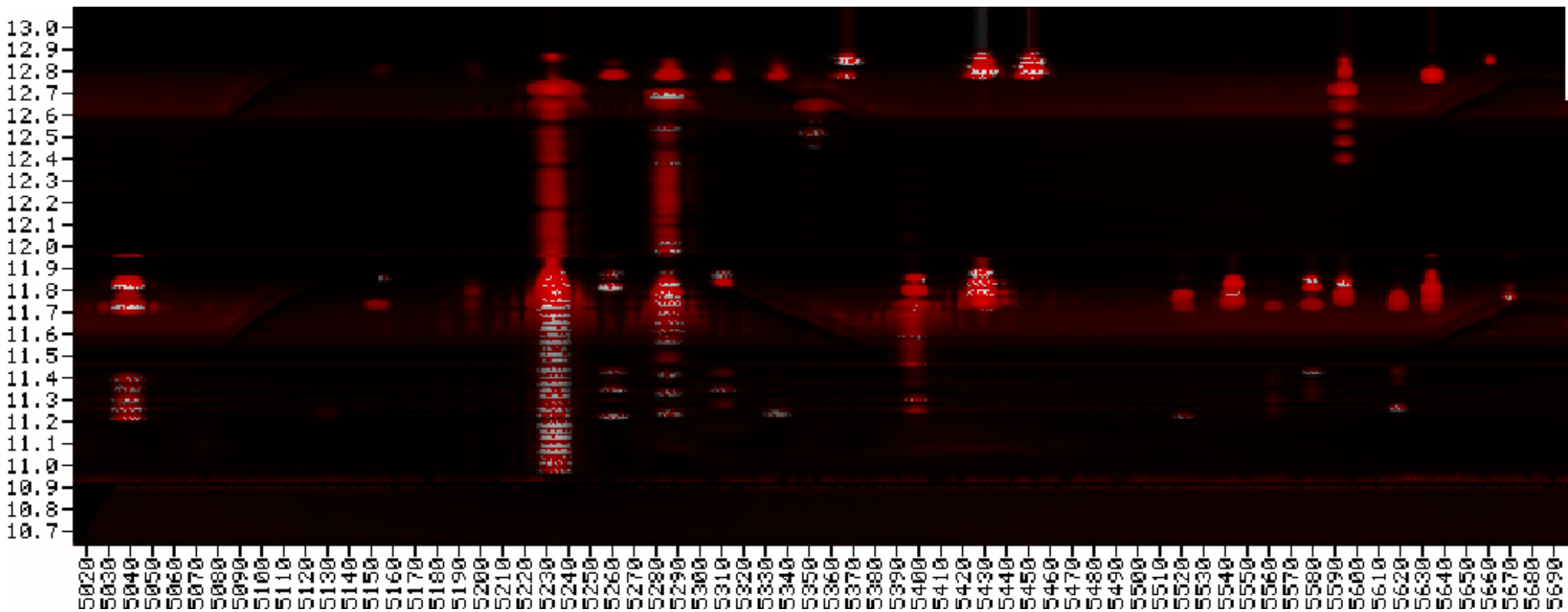
Visual Representations



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 Search

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

ZAP TIMERS CONTROL CONFIG HELP

ZAP: TV - Bouquets

TV	All Services	Satellites	Providers	Bouquets
Radio				
Data				
Movies				
Root				
Stream				
	Favourites (TV)			
	free	(0.0W) Premiere---Astra(19.2E)---		
	pr0n	(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

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

Tor Disabled

Stream Info

Applications Places System

Mon 4 Feb, 4:57 PM 9 °C

File Edit View History Bookmark

Google

http://192.168.111.67 - Stream Information - Mozilla Firefox

Stream Information	
Service Name	Ladbrokes Blackjack
Service Provider	BSkyB
Service Reference	1:0:82:c754:96b:2:11c0000:0:0:0:
VPID	ffffffffh (-1d)
APID	ffffffffh (-1d)
PCRPID	ffffffffh (-1d)
TPID	ffffffffh (-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

Done

Enigma Web Interfac... http://192.168.111.6... Starting Take Screen...

Tor Disabled

Stream Info

Applications Places System

File Edit View History Bookmarks

Google carling cup final

Enigma ... dvbsnoop p

Done

Enigma Web Interfac... http://192.168.111.6... Starting Take Screen...

Mon 4 Feb, 8:45 PM 8 °C

Tor Disabled

http://192.168.111.67 - Stream Information - Mozilla Firefox

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

carling cup final

Settings

enham H... Home | Carlin...

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

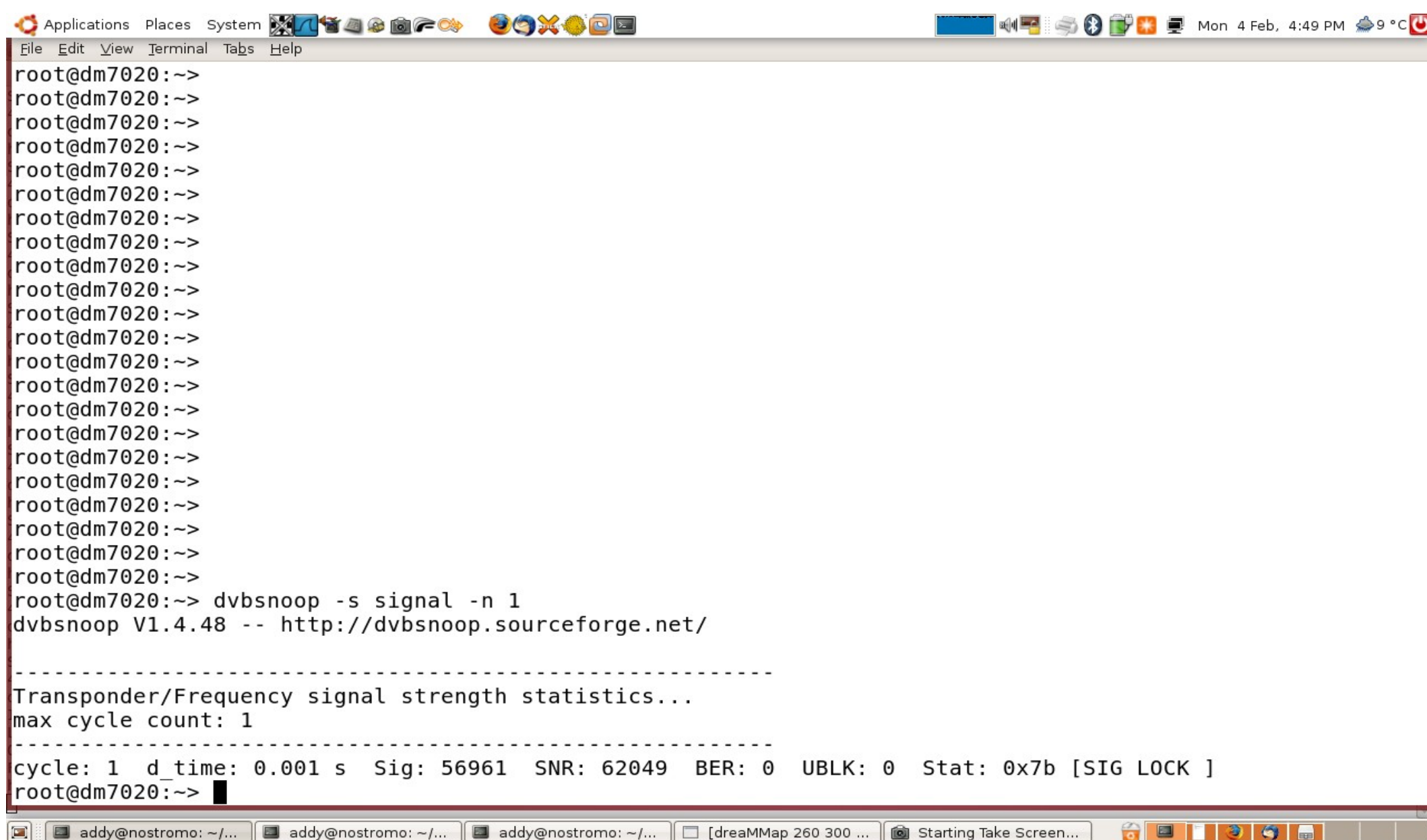


Stream Info

- 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



The image shows a terminal window with a menu bar (Applications, Places, System, File, Edit, View, Terminal, Tabs, Help) and a toolbar with various icons. The terminal output shows a series of 'root@dm7020:~>' prompts, followed by the command 'dvbsnoop -s signal -n 1'. Below this, the output of 'dvbsnoop V1.4.48' is shown, including a URL and statistics for a transponder. The terminal window is part of a desktop environment with a taskbar at the bottom showing several open windows.

```
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:~>
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

```
Applications Places System [Icons] [System Tray] Mon 4 Feb, 4:50 PM 9 °C
File Edit View Terminal Tabs Help

-----
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

```
Applications Places System [Icons] [System Tray] Mon 4 Feb, 4:50 PM 9 °C
File Edit View Terminal Tabs Help

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

Applications Places System
File Edit View Terminal Tabs Help

Mon 4 Feb, 4:52 PM 9 °C

```
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-behaved  
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
```

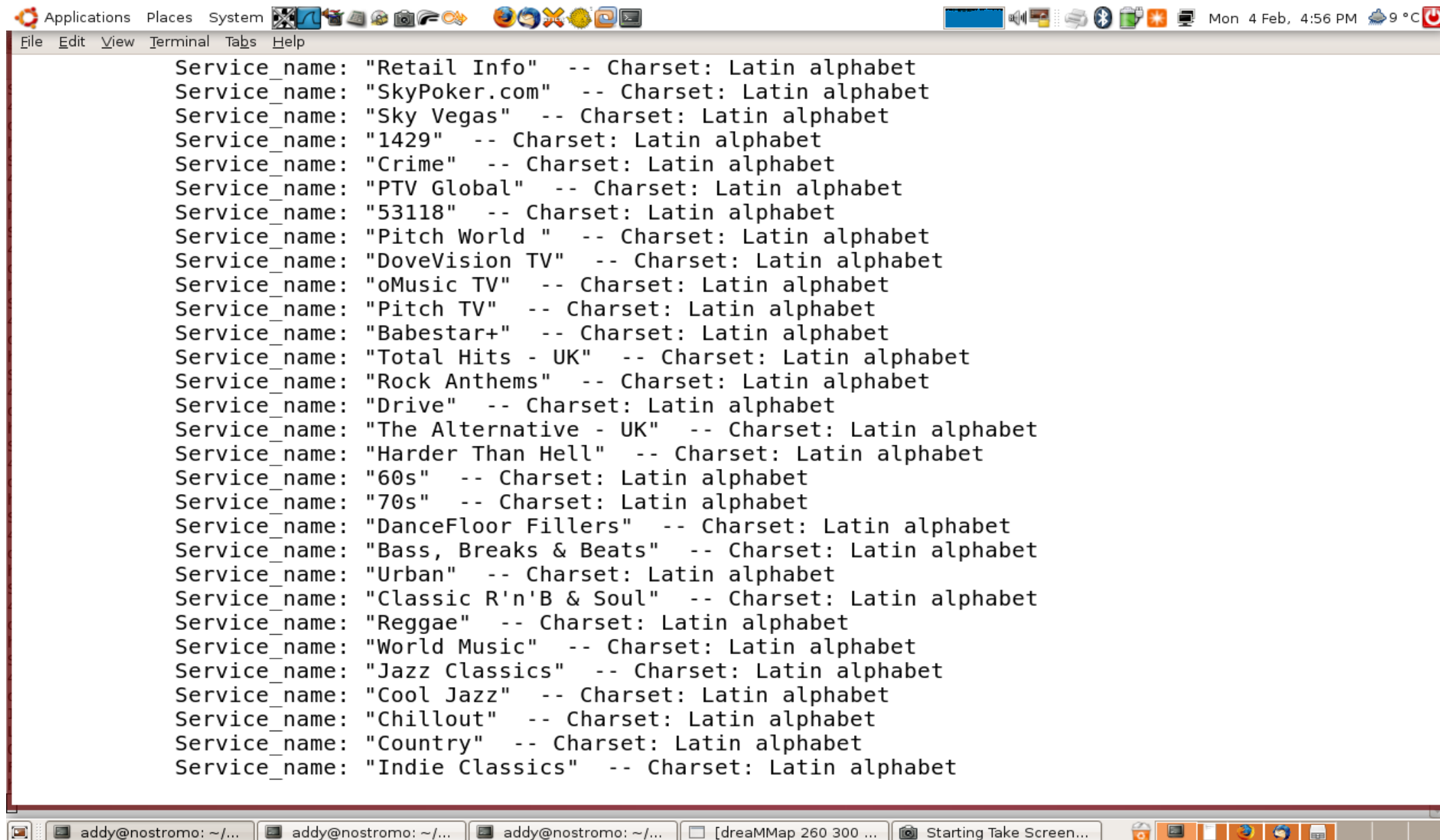
```
DVB-DescriptorTag: 80 (0x50) [= component_descriptor]
```

```
descriptor_length: 11 (0x0b)
```

```
reserved: 15 (0x0f)
```

addy@nostromo: ~/... addy@nostromo: ~/... addy@nostromo: ~/... [dreaMMap 260 300 ... Starting Take Screen...

Stream Info



The screenshot shows a Linux desktop environment. At the top, there is a menu bar with 'Applications', 'Places', and 'System'. Below it is a panel with various application icons. The main area is a terminal window displaying a list of service names and their character sets. The status bar at the bottom shows the date and time as 'Mon 4 Feb, 4:56 PM' and the temperature as '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 desktop environment includes a taskbar at the bottom with several open windows, including a terminal window, a file manager window, and a screen capture window. The terminal window is the active window, showing the output of a command that lists service names and their character sets.

Stream Info

```
Applications Places System [Icons] [System Tray] 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

```

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--

```

Stream Info

```

Applications  Places  System
File Edit View Terminal Tabs Help

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
    0010:  9f 6f a0 7a 5b ca bc c5 b5 17
    0020:  17 fe df cf a1 a7 2a 0d aa 3a
    0030:  b9 5f 48 5e 95 84 5b f4 2f d1
    0040:  75 20 14 f5 08 44 10 57 c1 2d
    0050:  8c ff 10 5a c5 7b a8 64 13 95
    0060:  a6 f6 f1 84 71 4d 97 1a 1a cc

--More--

```

Mon 4 Feb, 5:49 PM 8 °C

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

Stream Info

```
Applications Places System [Icons] [System Tray] Mon 4 Feb, 8:35 PM 8 °C
add@nostromo: ~/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)
=====

-----
add@nostromo: ~/... add@nostromo: ~/... 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

Applications Places System

Enigma Web Interface - Dreambox - Mozilla Firefox

File Edit View History Bookmarks Tools Help

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

satellite feed hunter dx

Google satellite feed hunter dx

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

DREAM multimedia

SNR: 92% AGC: 87% BER: 0 locked 224:07 h up 192.168.111.67 vpid: none apid: none

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

0:00

ZAP TIMERS CONTROL CONFIG HELP

ZAP: TV - Satellites

TV	All Services	Satellites	Providers	Bouquets
Radio	Astra (19.2E) - new found			
Data	Astra (19.2E) - services			
Movies	Astra/Eurobird (28.2E) -			
Root	Astra/Eurobird (28.2E) -			
Stream	Eutelsat W2 (16.0E) - ne			
	Eutelsat W2 (16.0E) - se			
	Hotbird (13.0E) - new fo			
	Hotbird (13.0E) - service			
	current transponder			
	(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			
	(19.2E) ENCYCLOPEDIA			

Done

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

Tor Disabled

Taking over the Dreambox

Applications Places System

Enigma Web Interface - Dreambox - Mozilla Firefox

File Edit View History Bookmarks Tools Help

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

Google Search

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

100% Babes

DREAM multimedia

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

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

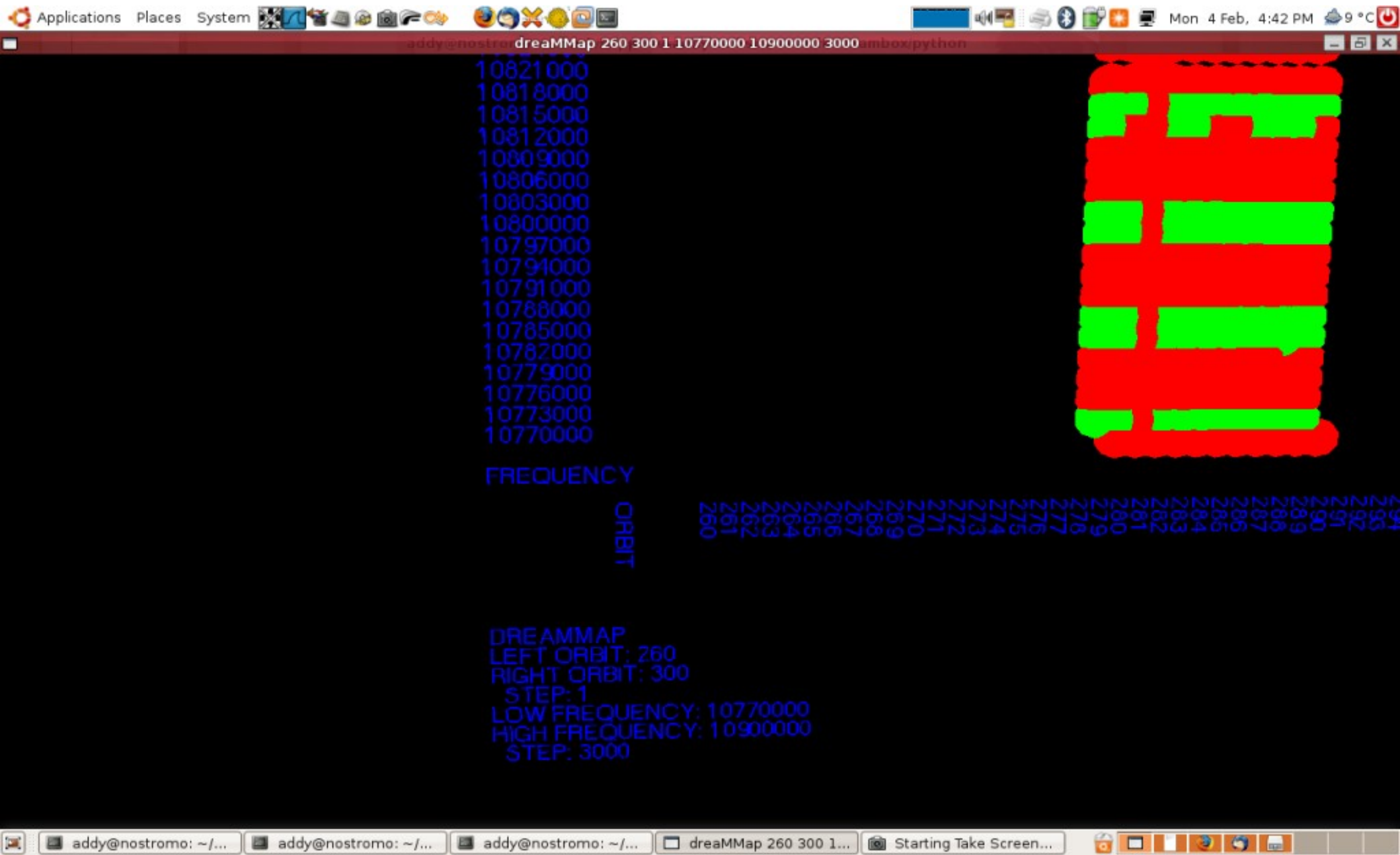
Enigma Web Interfac... Starting Take Screen...

Tor Disabled

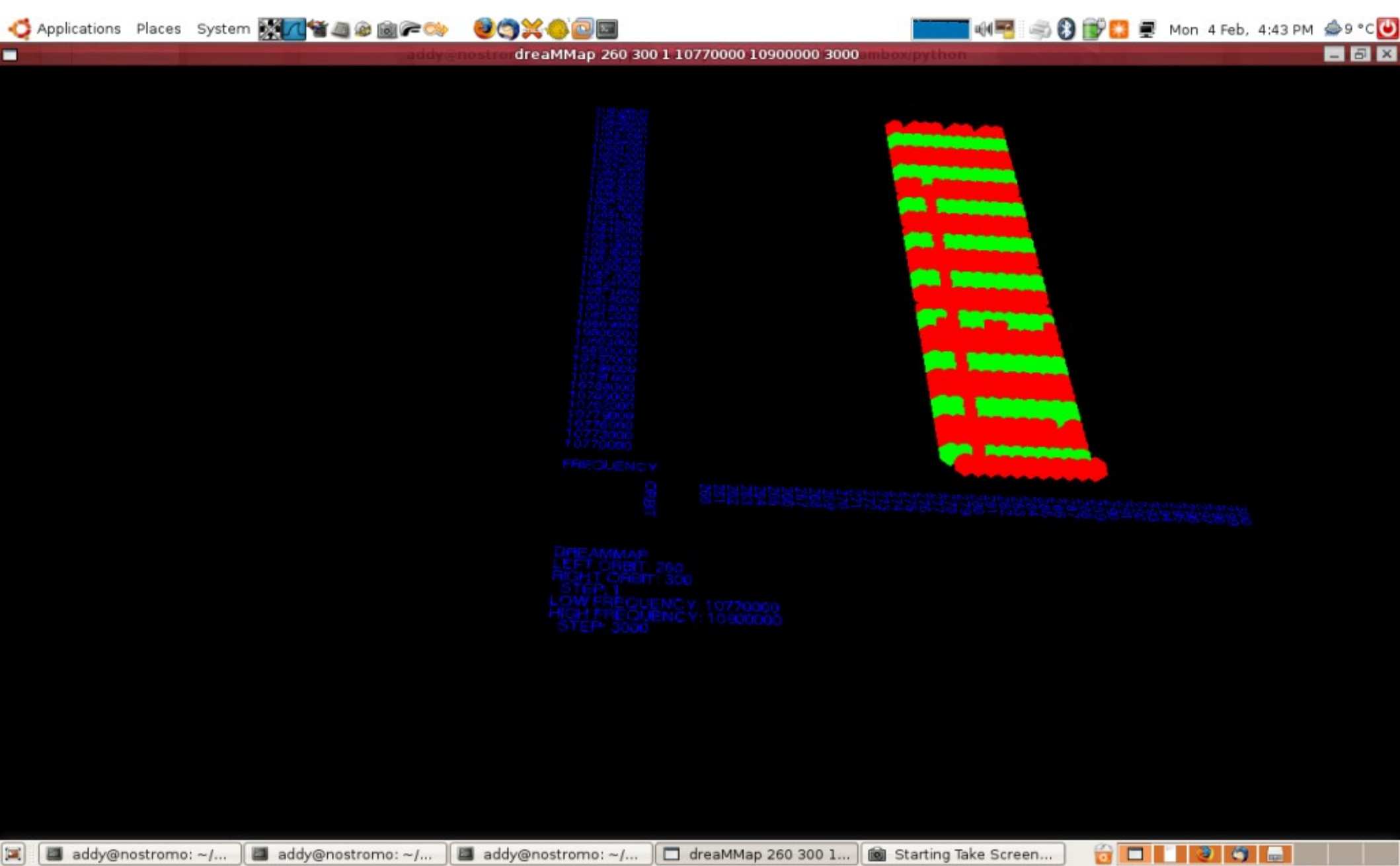
dreMap

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

This is now...



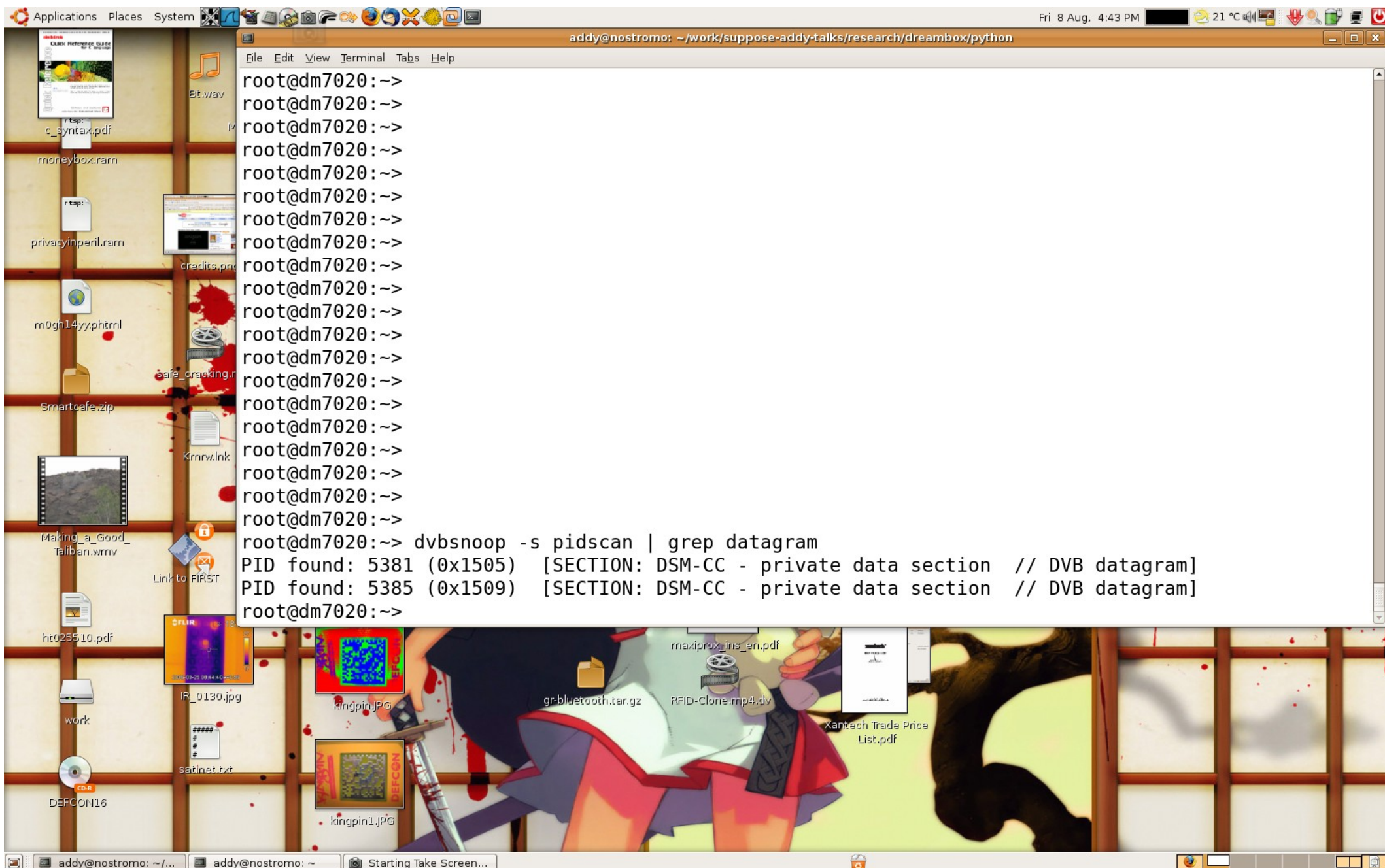
This is now...



3D model capabilities

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

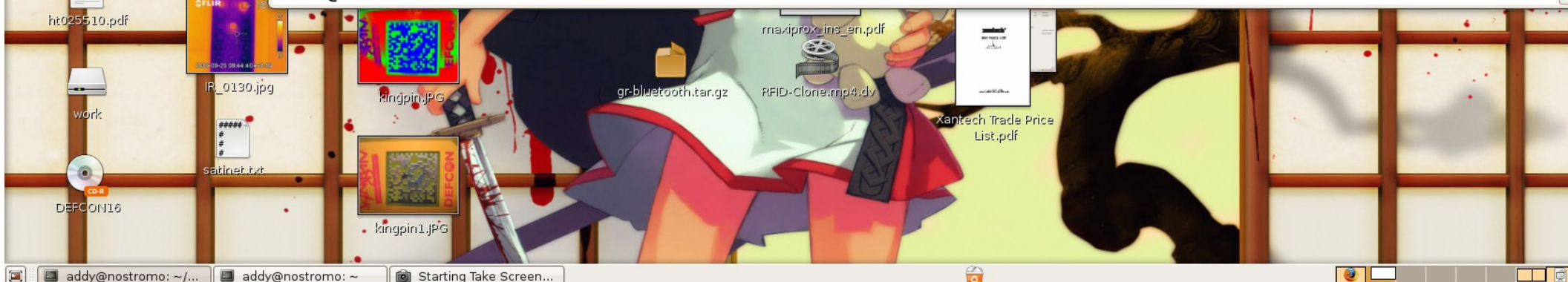
Demonstration

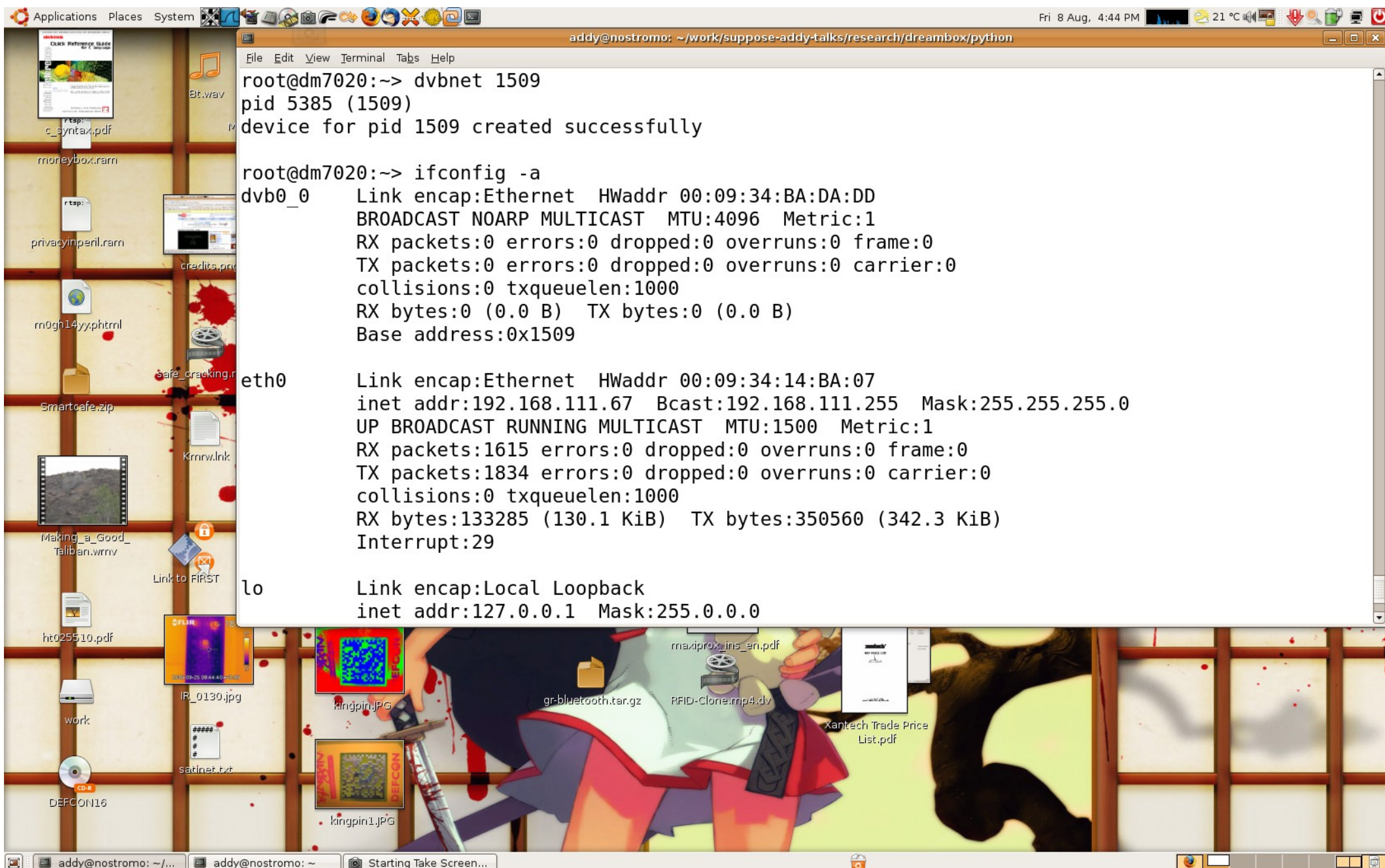


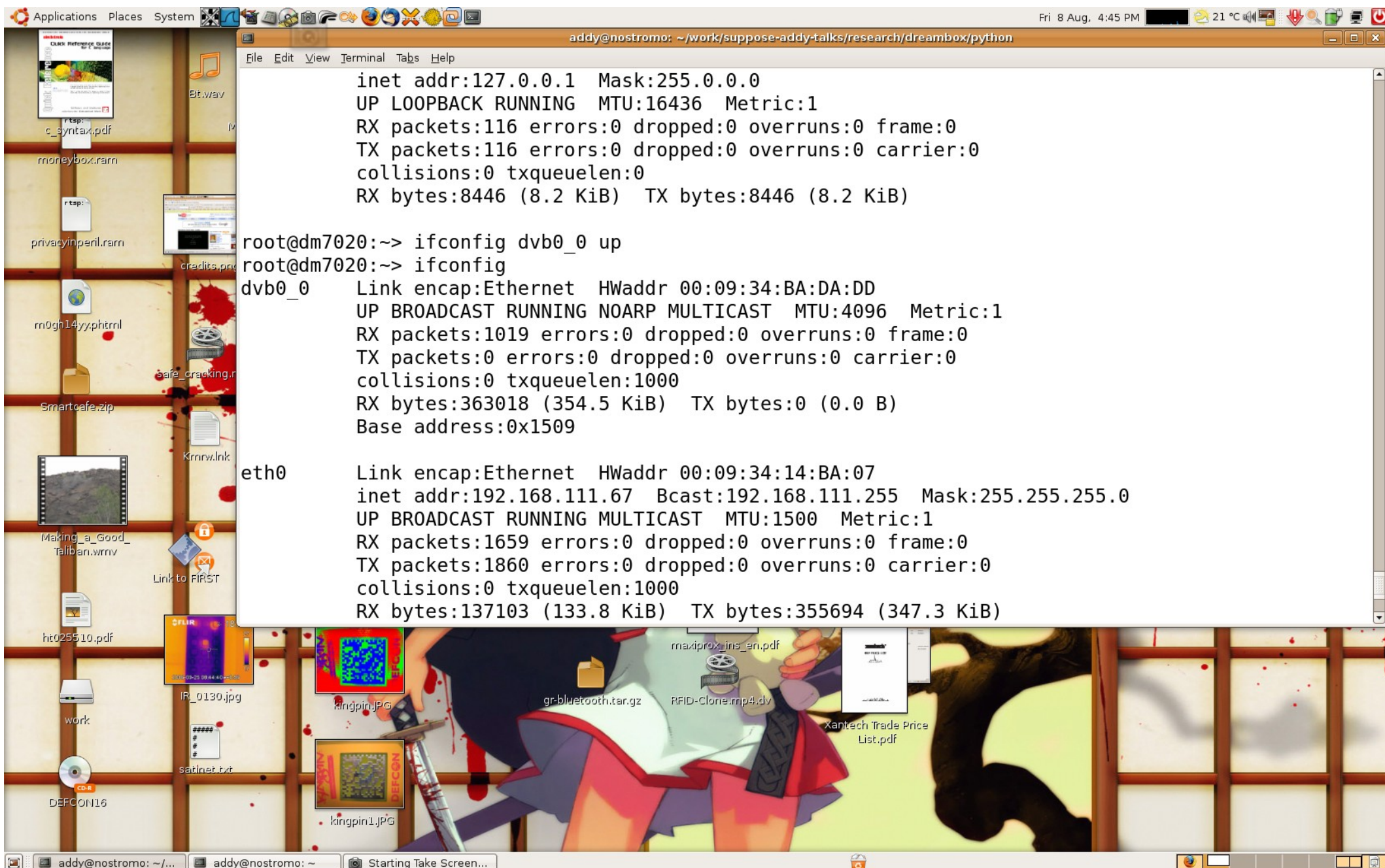
File Edit View Terminal Tabs Help

```
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:~> 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:~>
```





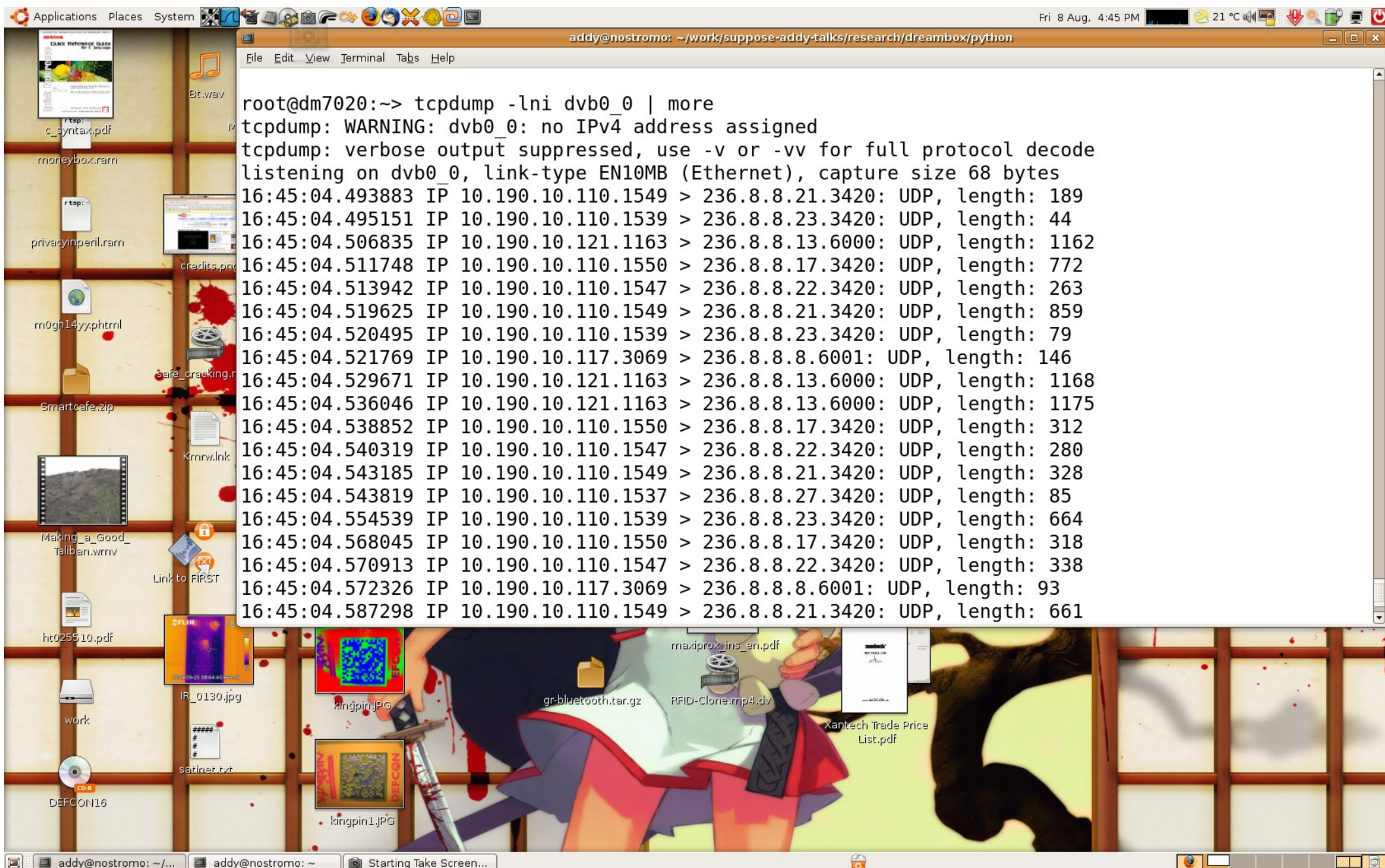


```
addy@nostromo: ~/work/suppose-addy-talks/research/dreambox/python
File Edit View Terminal Tabs Help

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)
```



Equipment List

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

Questions?

<http://rfidiot.org>

adam@algroup.co.uk