Leonardo Nve Egea
lnve@s21sec.com

Playing in a Satellite environment 1.2

Why 1.2?

1. because I'm sure that some people will publish more attacks.

.2 because previously presentations about satellite.

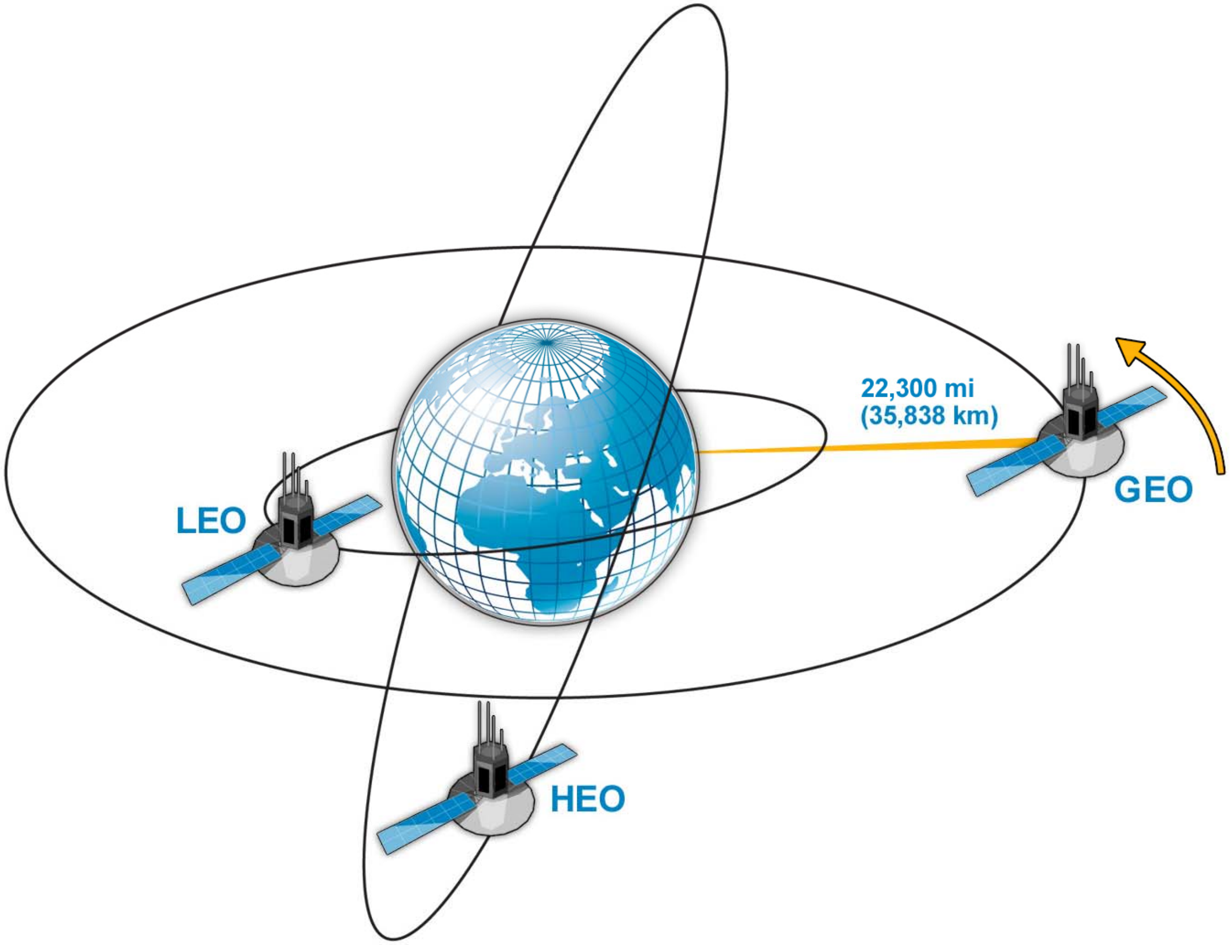
Who comented this before?

- Warezzman – (in 2004 at Undercon VIII first Spanish hacker CON)
- Jim Geovedi & Raditya Iryandi (HITBSecConf2006)
- Adam Laurie (Blackhat 2009 at DC)
- Myself at S21Sec Blog (February 2009)

Intro to SAT

- Orbit based satellites
  - Low Earth orbiting (LEO)
  - Geostationary orbit (GEO)
  - Other: Molniya, High (HEO), etc.
- Function based satellites
  - Communications
  - Earth observation
  - Other: Scientifics, ISS, etc.

Intro to SAT



Intro to SAT

- Satellite LEO
  - Meteorological
  - HAM (Amateur Radio Operator)

- Satellite GEO
  - UFO (UHF Follow ON) Military
  - Inmarsat
  - Meteorological (Meteosat)
  - SCPC / Telephony link FDMA

[redacted]

DVB®

Digital Video
Broadcasting

The signal from the sky you ever waiting

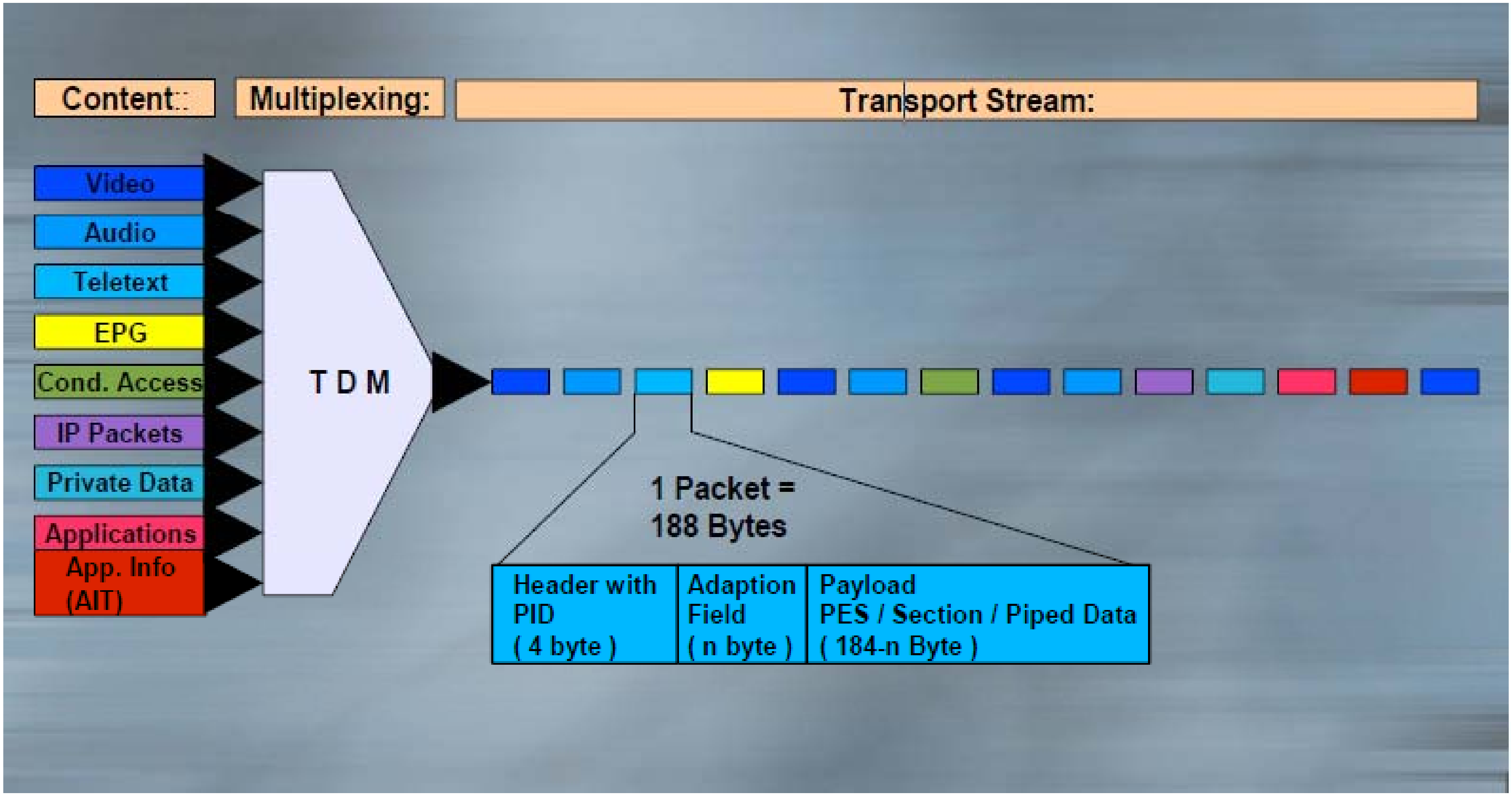
DVB

- Standard of European Telecommunications Standards Institute (ETSI).
- Defines audio and video transmission, and data connections.
- DVB-S & DVB-S2 is the specification for satellite communications.

DVB-S

- Transponder: Like channels (in Satellite comms)
  - Frecuency (C band or Ku). Ex: 12.092Ghz
  - Polarization. (horizontal/vertical)
  - Symbol Rate. Ex: 27500Kbps
  - FEC.
- Every satellite has many transponders onboard which are operating on different frequencies

DVB-S


Content::
Multiplexing:
Transport Stream:
Video
Audio
Teletext
EPG
Cond. Access
IP Packets
Private Data
Applications
App. Info (AIT)
T D M
1 Packet = 188 Bytes
Header with PID (4 byte)
Adaption Field (n byte)
Payload PES / Section / Piped Data (184-n Byte)

DVB-S

Header				Body	
0x47	Flags	PID	Flags	Adaptation Field	Data

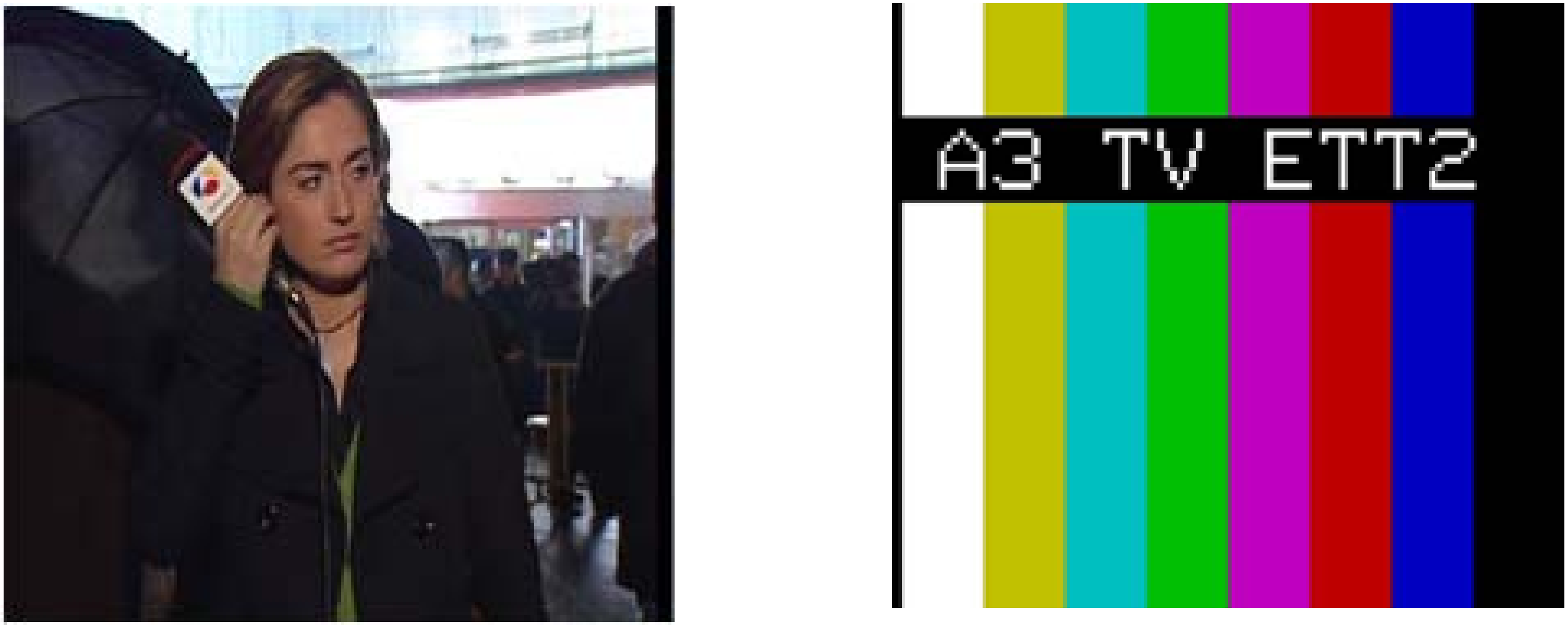
Program ID (PID): It permits different programs at same transponder with different components [Example BBC1 PIDs: 600 (video), 601 (English audio), 603 (subtitles), 4167 (teletext)]

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

DVB Feeds

- Temporal video links.
- Live emissions, sports, news.
- FTA – In open video.

DVB Feeds

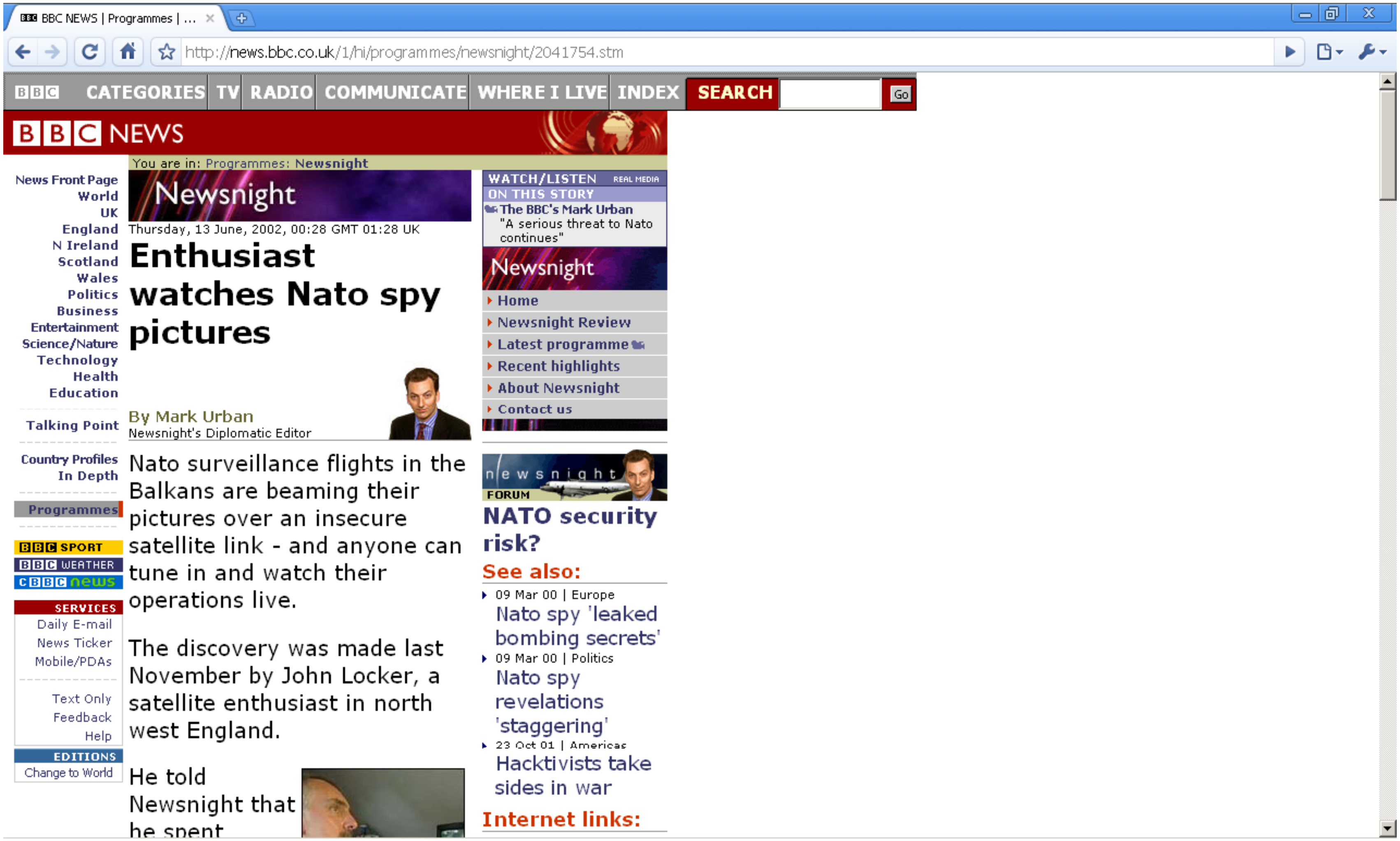


Hispasat Pre news feed (live news)

DVB Feeds

ATLAS Agency to TV feeds

DVB Feeds (2002)



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

The BBC's Mark Urban
"A serious threat to Nato continues"

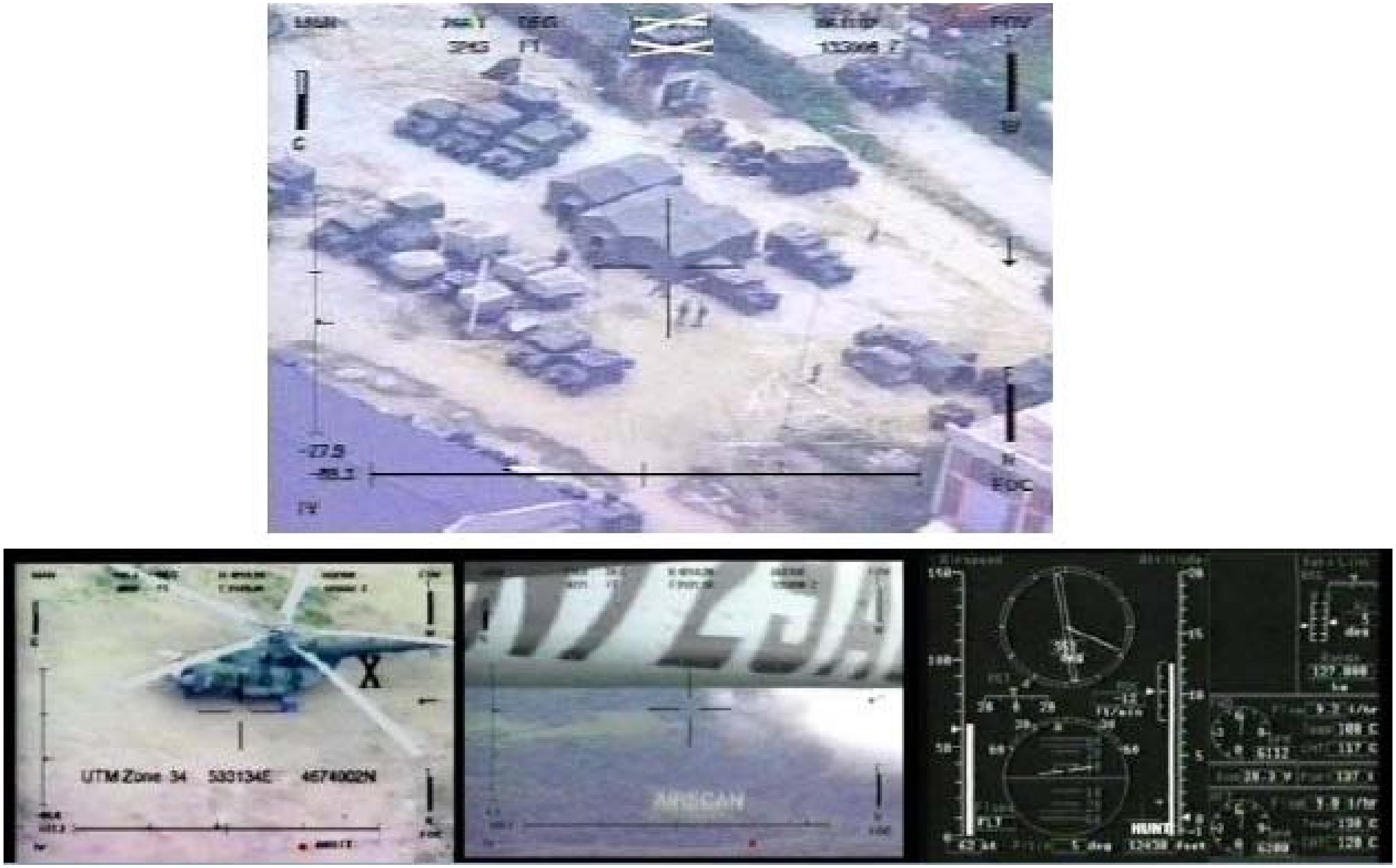
NATO security risk?

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:

DVB Feeds (2002)



Captured NATO feeds

DVB Feeds (2002)

NATO COMINT official

DVB Feeds

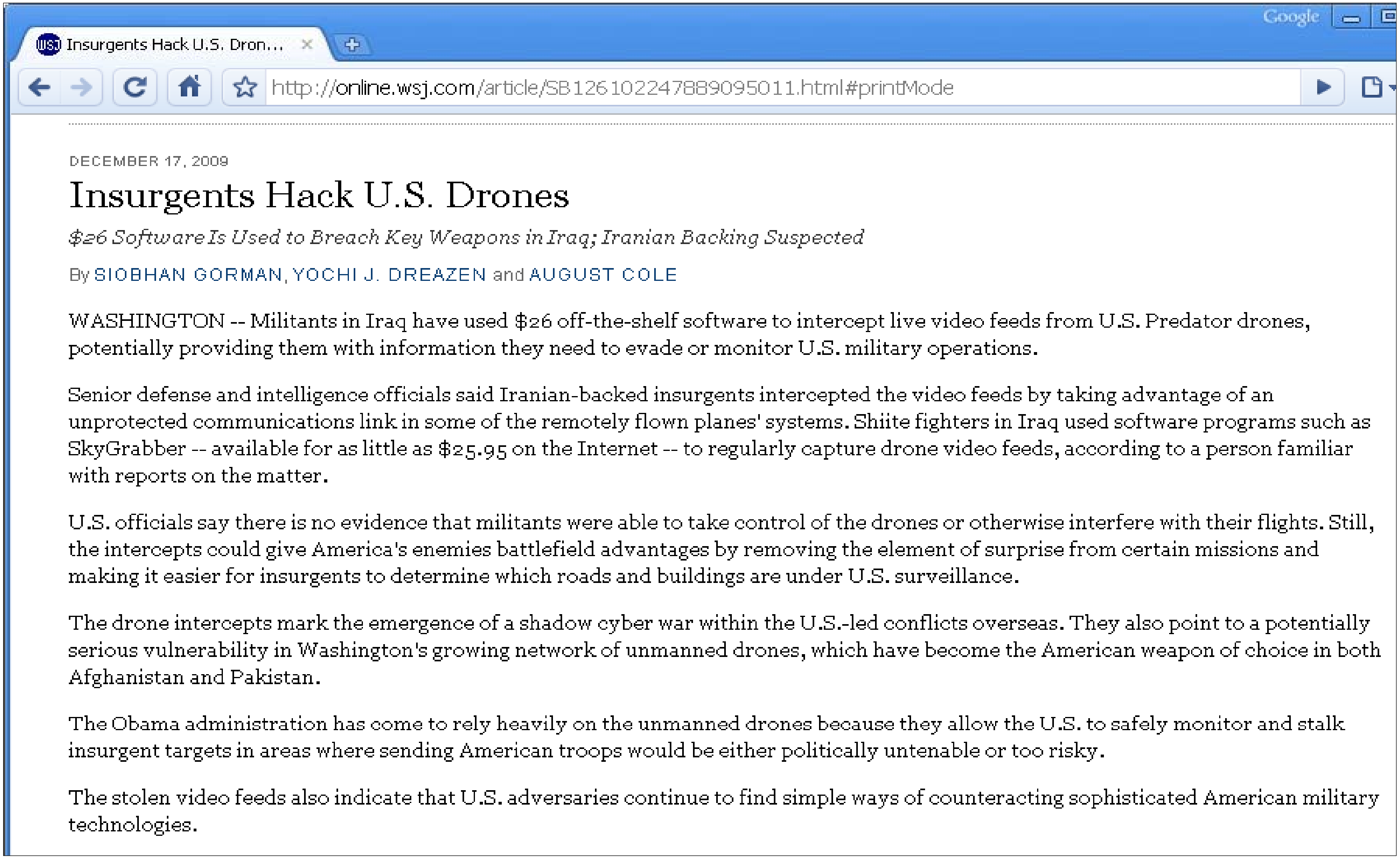
- I widely known that the Department of Defense (DoD) and some US defense contractors use satellites and DVB for their comms.

DVB Feeds

- Let`s see:

http://telecom.esa.int/telecom/media/document/DVB-RCS%20Networks%20for%20the%20US%20Defense%20Market%20(R3).pdf

DVB Feeds (2009)


Insurgents Hack U.S. Dron...
Google
http://online.wsj.com/article/SB126102247889095011.html#printMode

DECEMBER 17, 2009

Insurgents Hack U.S. Drones

$26 Software Is Used to Breach Key Weapons in Iraq; Iranian Backing Suspected

By SIOBHAN GORMAN, YOCHI J. DREAZEN and AUGUST COLE

WASHINGTON -- Militants in Iraq have used $26 off-the-shelf software to intercept live video feeds from U.S. Predator drones, potentially providing them with information they need to evade or monitor U.S. military operations.

Senior defense and intelligence officials said Iranian-backed insurgents intercepted the video feeds by taking advantage of an unprotected communications link in some of the remotely flown planes' systems. Shiite fighters in Iraq used software programs such as SkyGrabber -- available for as little as $25.95 on the Internet -- to regularly capture drone video feeds, according to a person familiar with reports on the matter.

U.S. officials say there is no evidence that militants were able to take control of the drones or otherwise interfere with their flights. Still, the intercepts could give America's enemies battlefield advantages by removing the element of surprise from certain missions and making it easier for insurgents to determine which roads and buildings are under U.S. surveillance.

The drone intercepts mark the emergence of a shadow cyber war within the U.S.-led conflicts overseas. They also point to a potentially serious vulnerability in Washington's growing network of unmanned drones, which have become the American weapon of choice in both Afghanistan and Pakistan.

The Obama administration has come to rely heavily on the unmanned drones because they allow the U.S. to safely monitor and stalk insurgent targets in areas where sending American troops would be either politically untenable or too risky.

The stolen video feeds also indicate that U.S. adversaries continue to find simple ways of counteracting sophisticated American military technologies.

DVB Feeds (2009)

US COMINT official

DVB Feeds

- Find feeds:
    - Lists of channels in www
    - Blind Scan
    - Visual representations of the signal

DVB Feeds - Too know more

- Dr HANS
  - http://drhans.jinak.cz/news/index.php

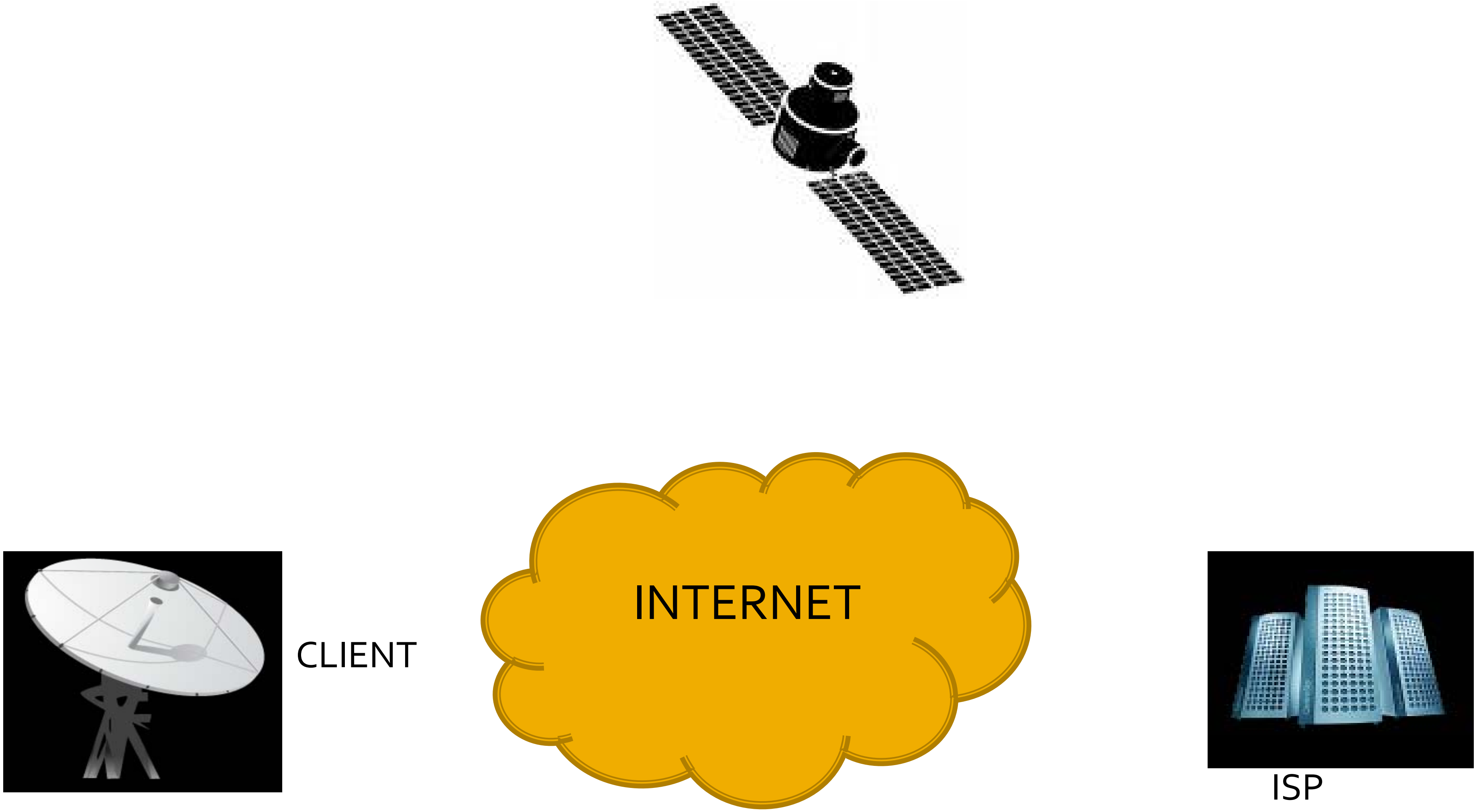
- Zackyfiles
  - http://www.zackyfiles.com (in spanish)

- Satplaza
  - http://www.satplaza.com

DVB Data

- Two scenarios
  - Satmodem
  - Satellite Interactive Terminal (SIT) or Astromodem

DVB Data - Satmodem

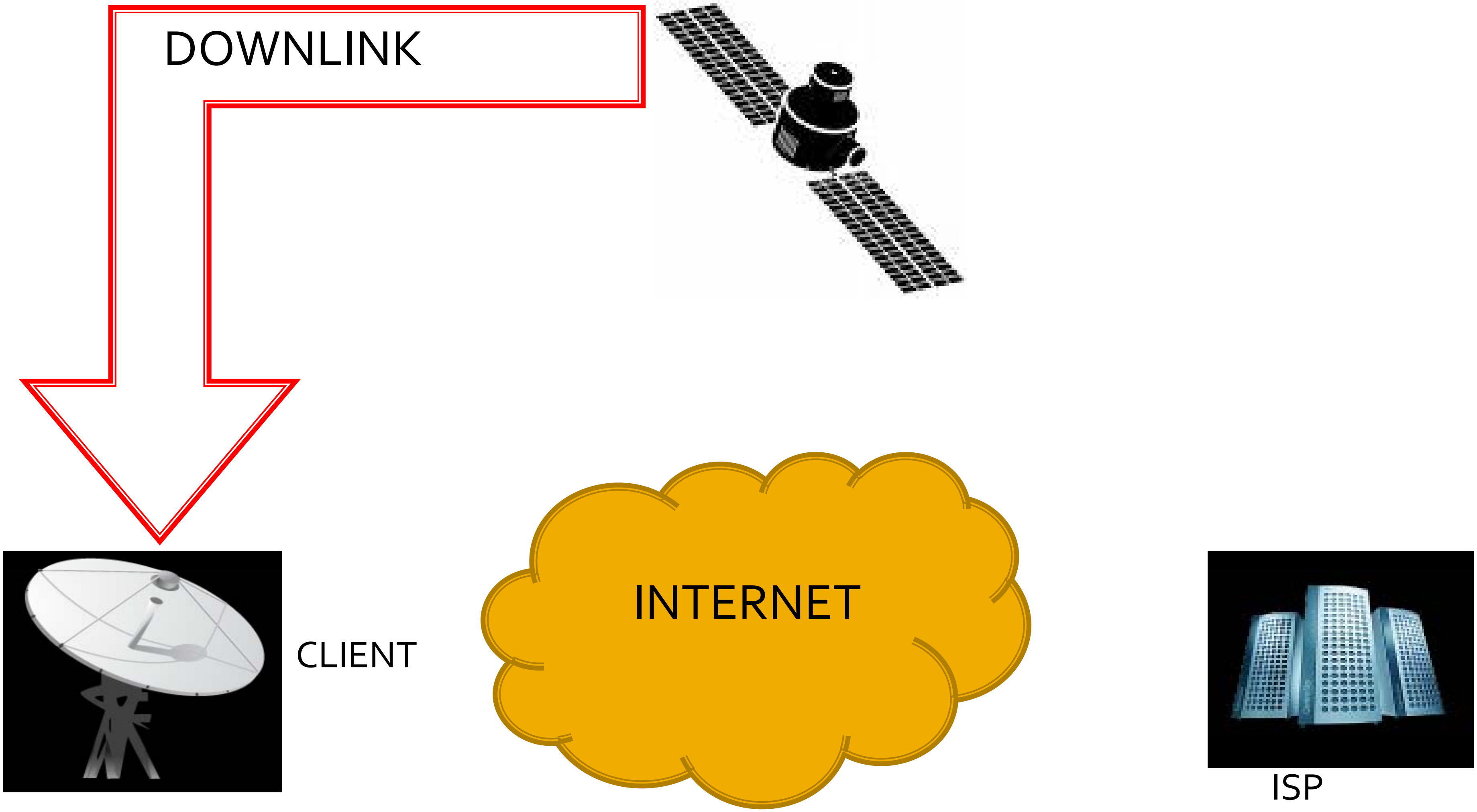


INTERNET

CLIENT

ISP

DVB Data - Satmodem



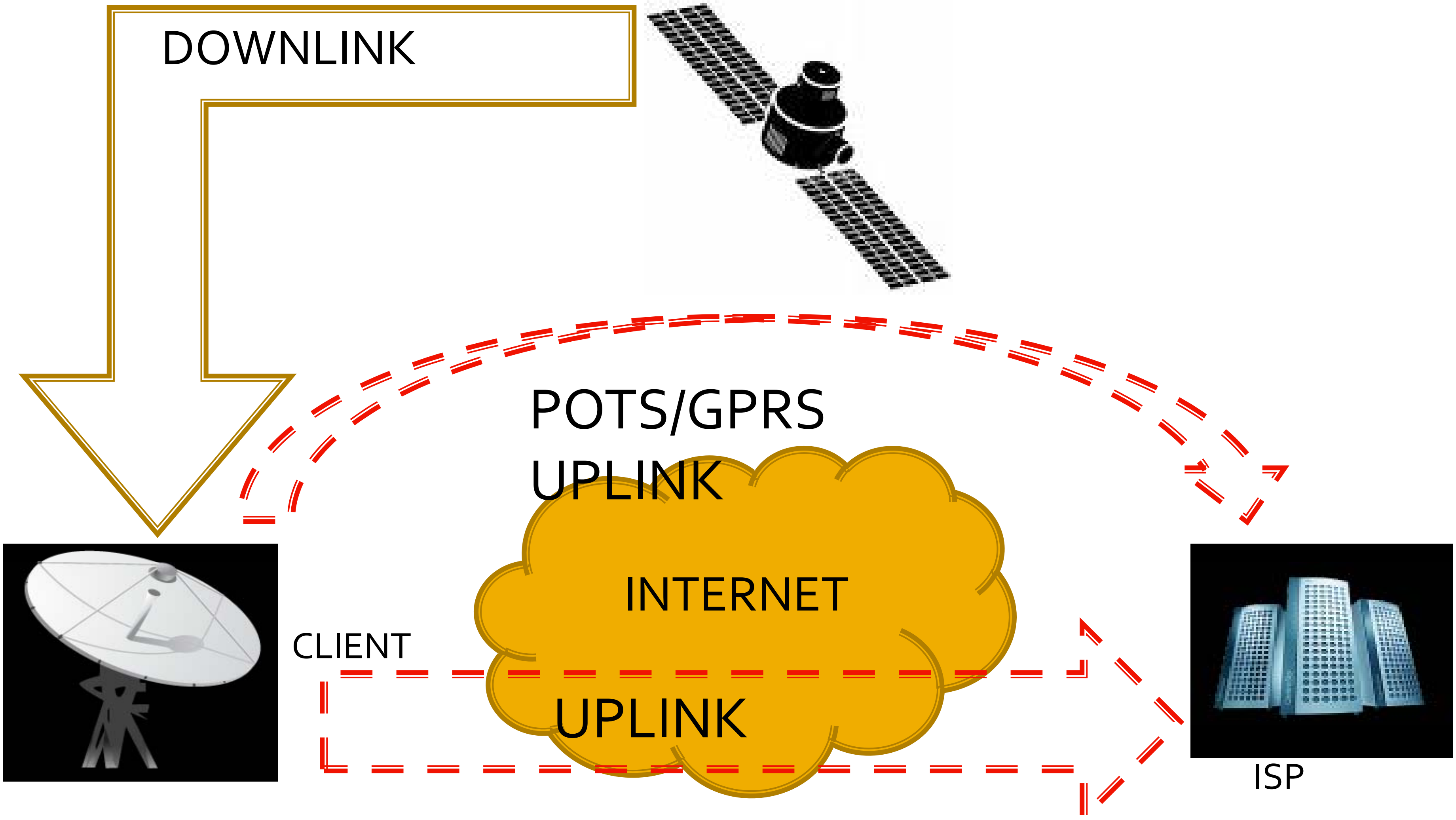
DOWNLINK

CLIENT

INTERNET

ISP

DVB Data - Satmodem



DOWNLINK

POTS/GPRS UPLINK

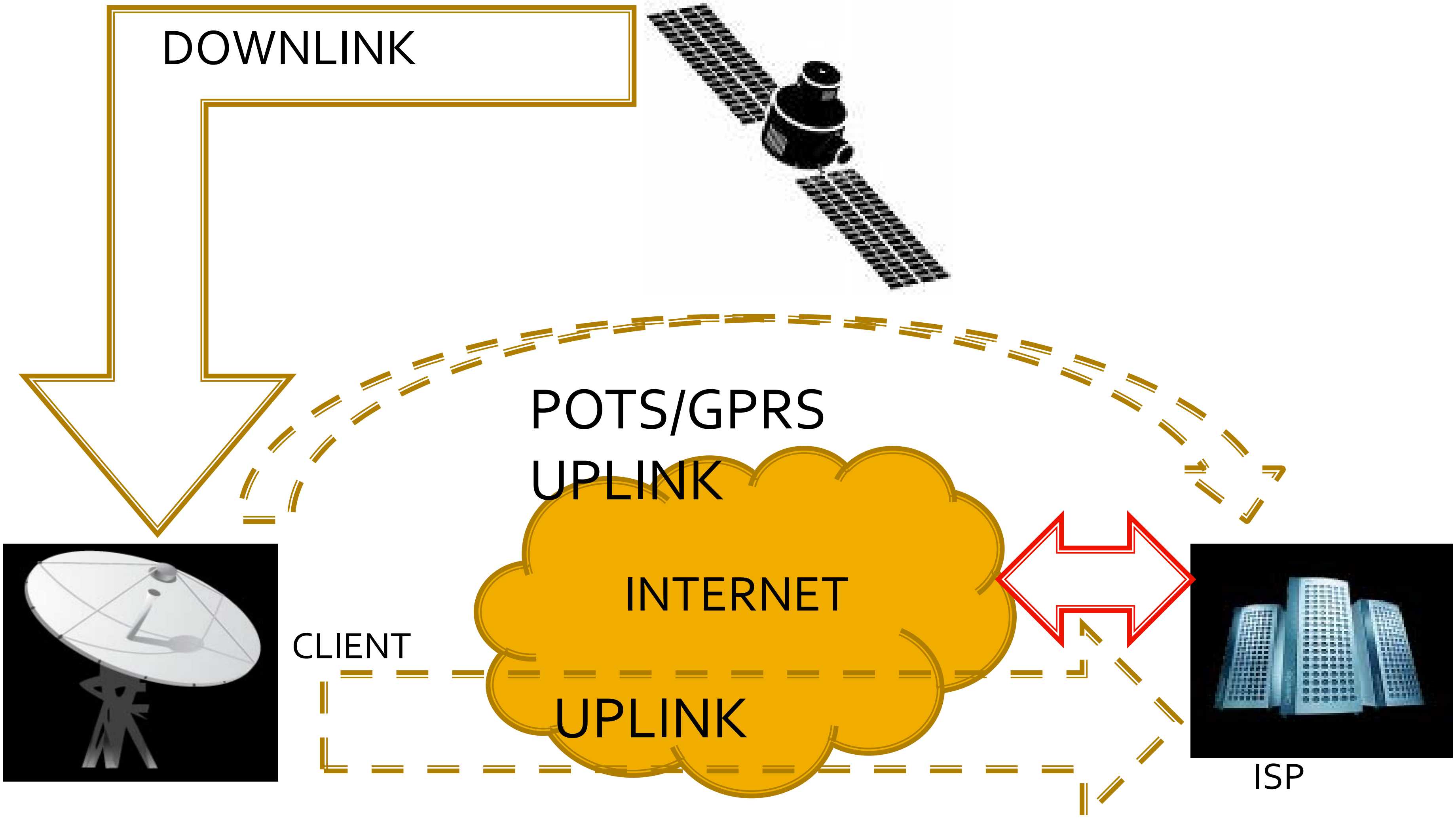
INTERNET

CLIENT

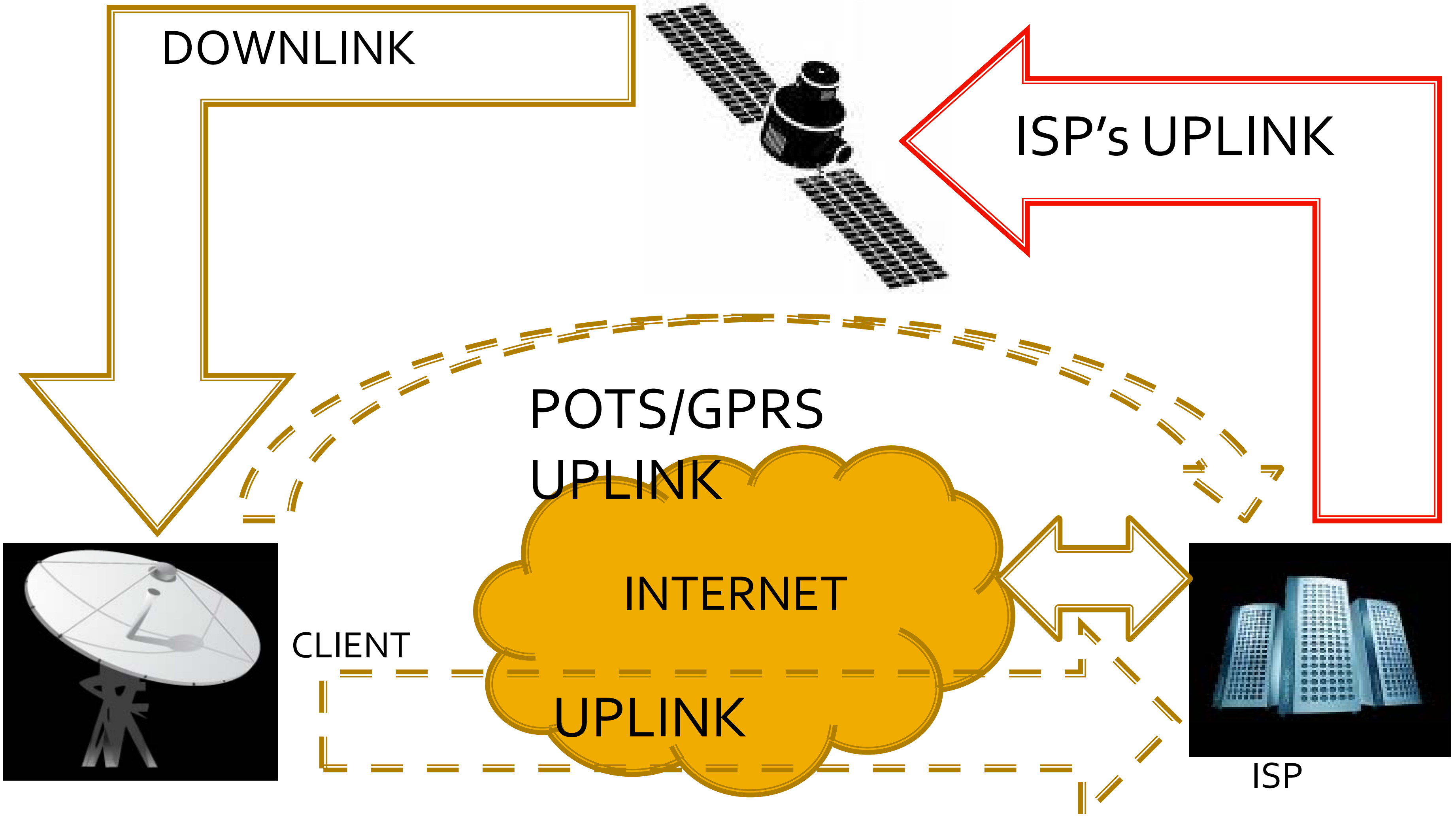
UPLINK

ISP

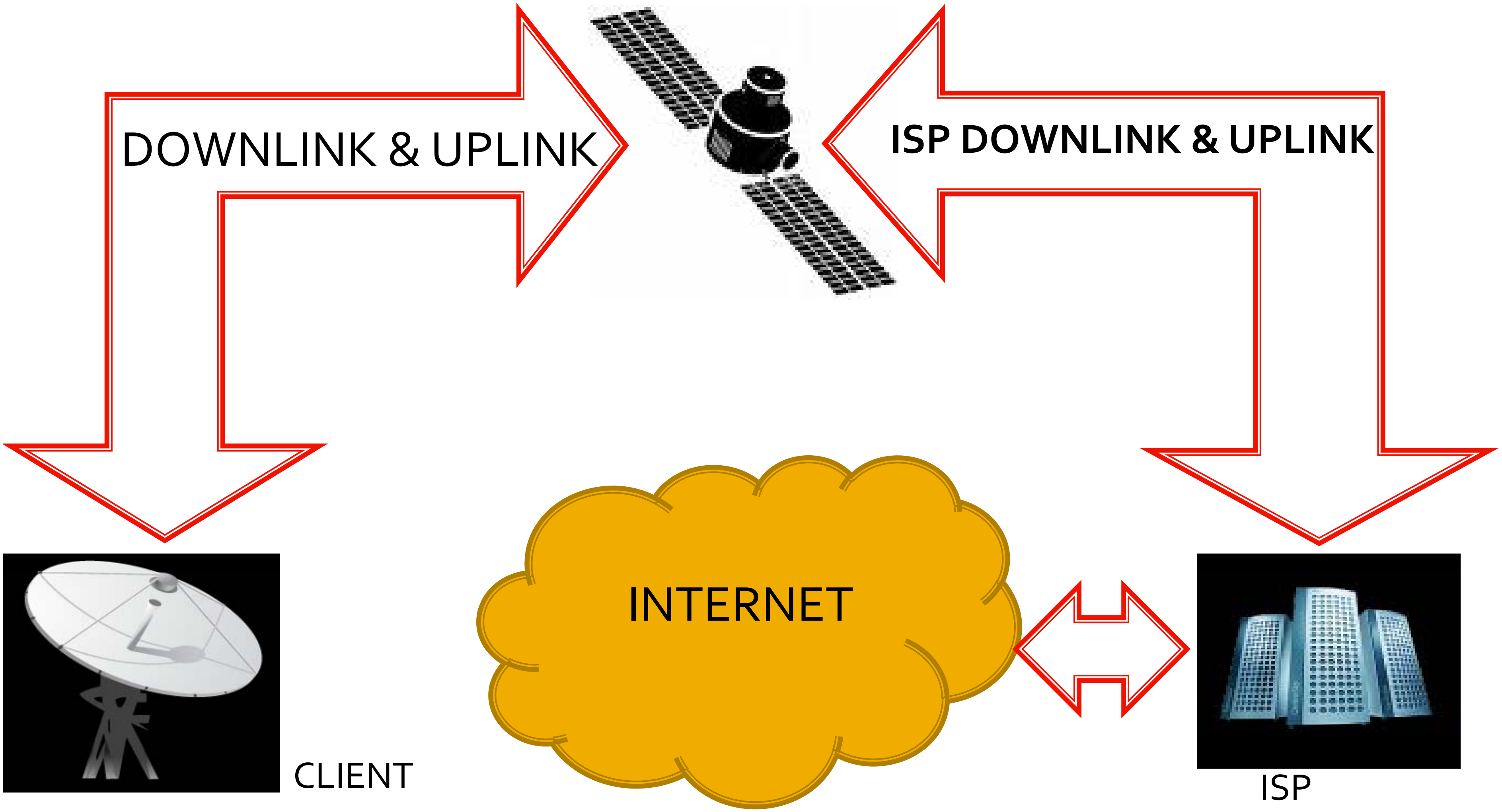
DVB Data - Satmodem



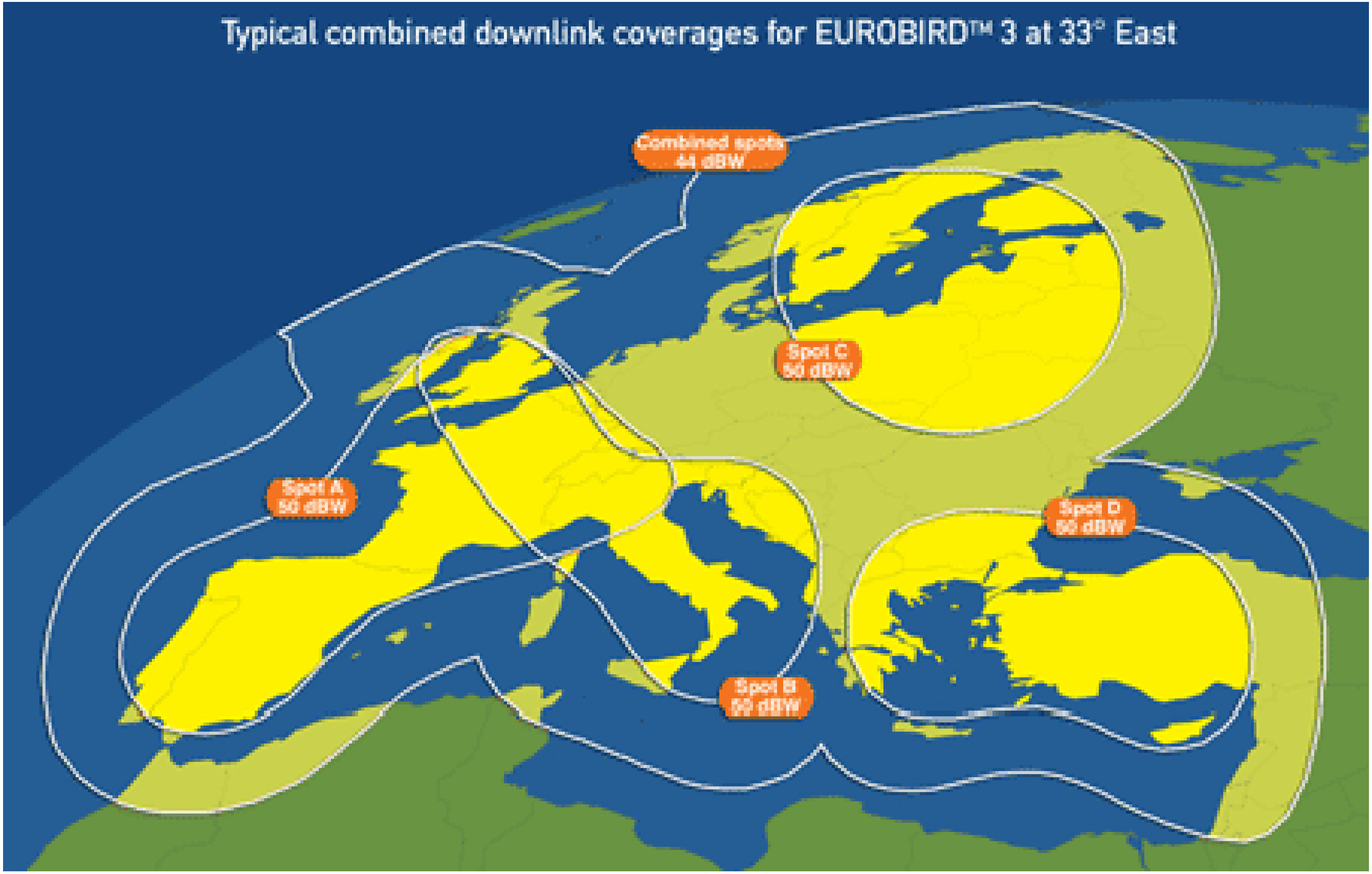
DVB Data - Satmodem



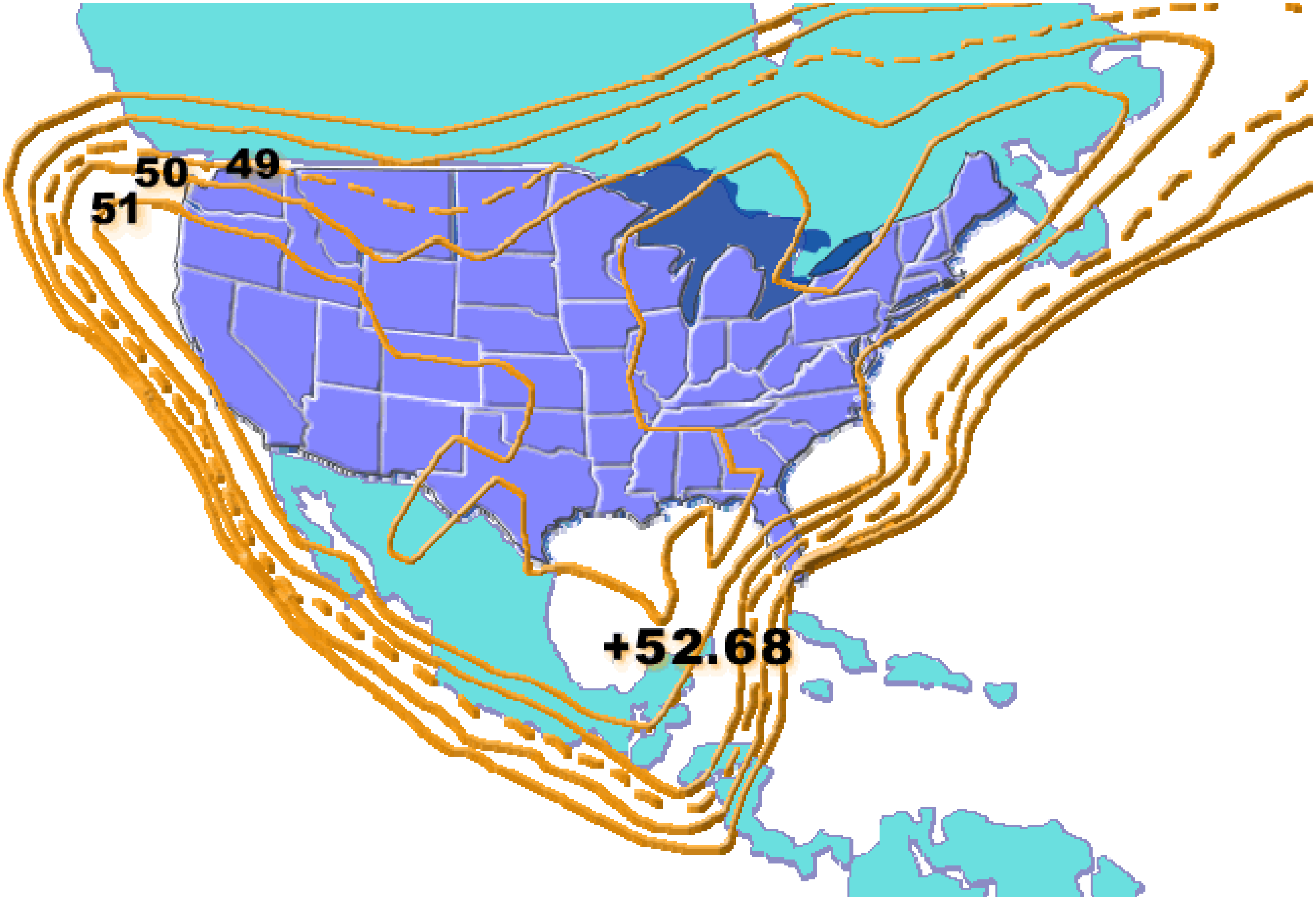
DVB Data - Astromodem



Satellite Coverage



Satellite Coverage



DVB Data

Anyone with coverage can SNIFF the DVB Data, and normally it is unencrypted.

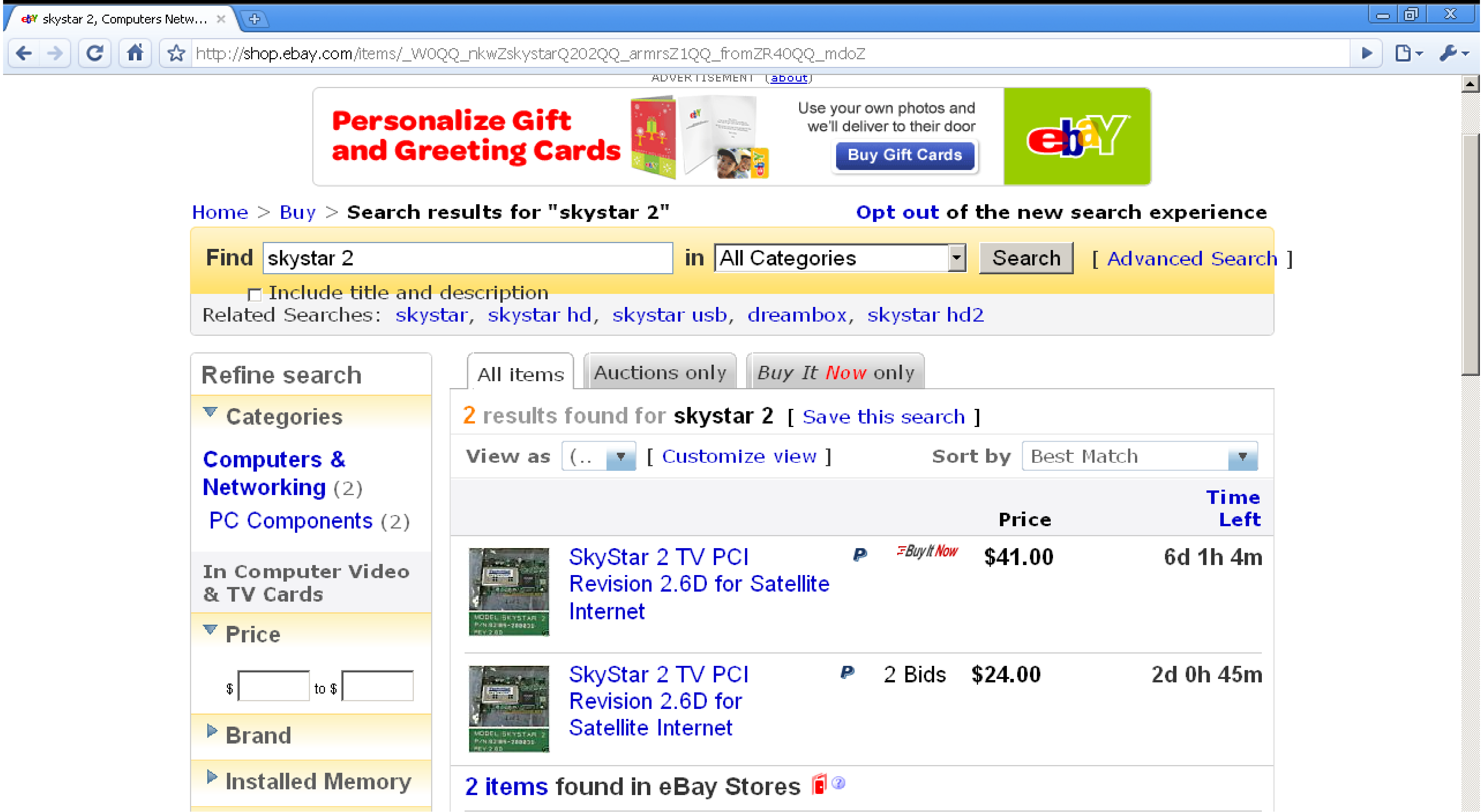
DVB Data

- What do you need:
  - Skystar 2 DVB Card
  - linuxtv-dvb-apps
  - Wireshark
  - The antenna
  - Data to point it.

DVB Data

I bought it for 50€!!! from an PayTV ex-"hacker" :P (Including a set-top box that I will not use)

DVB Data



skystar 2, Computers Netw...

http://shop.ebay.com/items/_W0QQ_nkwZskystarQ202QQ_armrsZ1QQ_fromZR40QQ_mdoZ

Home > Buy > Search results for "skystar 2"

Opt out of the new search experience

Find skystar 2 in All Categories Search [Advanced Search]

□ Include title and description

Related Searches: skystar, skystar hd, skystar usb, dreambox, skystar hd2

Refine search

Categories

Computers & Networking (2)

PC Components (2)

In Computer Video & TV Cards

Price

$ to $

Brand

Installed Memory

All items | Auctions only | *Buy It Now* only

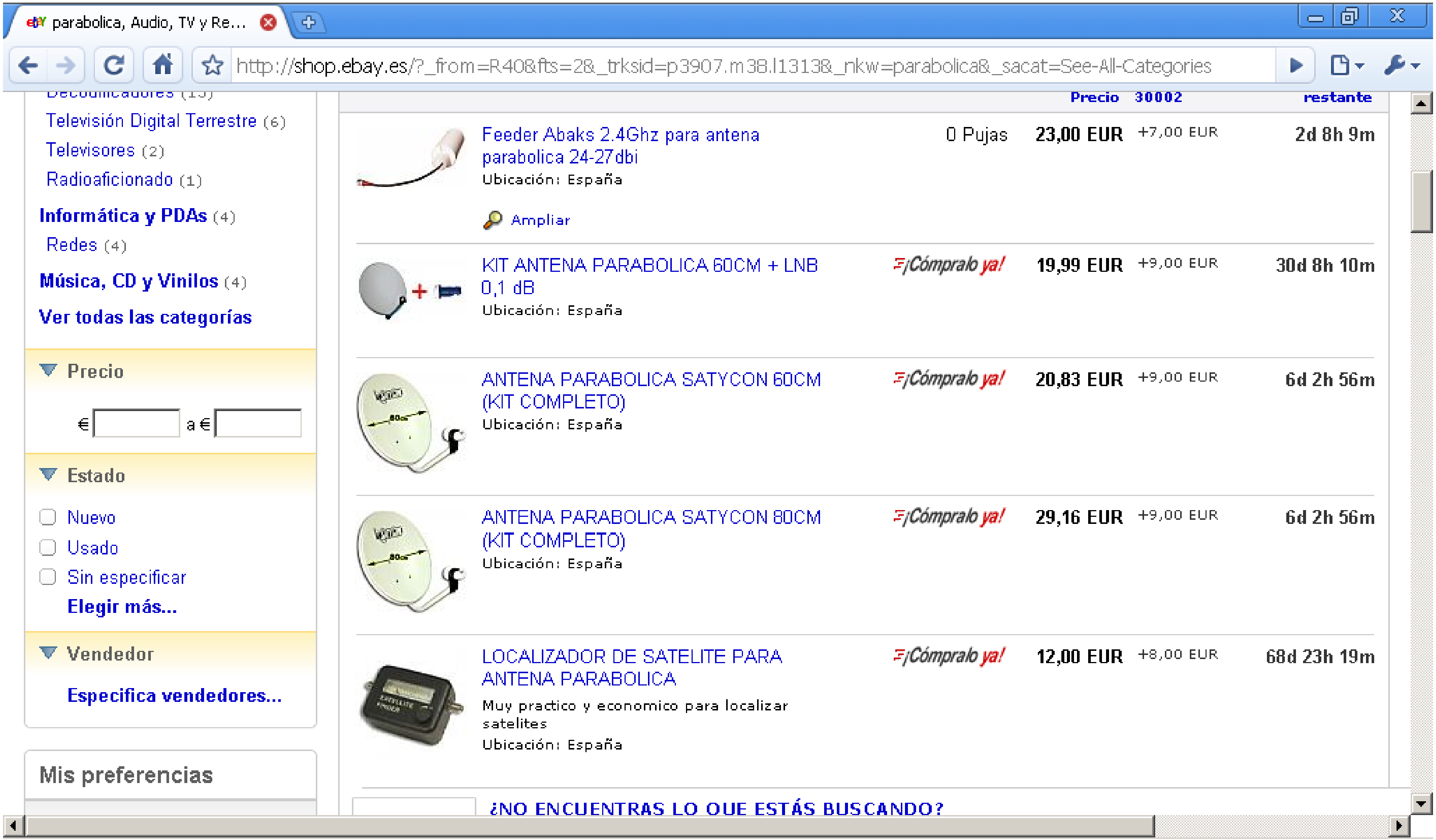
2 results found for **skystar 2** [Save this search]

View as (.. [Customize view] Sort by Best Match

			Price	Time Left
SkyStar 2 TV PCI Revision 2.6D for Satellite Internet	P	Buy It Now	$41.00	6d 1h 4m
SkyStar 2 TV PCI Revision 2.6D for Satellite Internet	P	2 Bids	$24.00	2d 0h 45m

2 items found in eBay Stores

DVB Data



parabolica, Audio, TV y Re...

http://shop.ebay.es/?_from=R40&fts=2&_trksid=p3907.m38.l1313&_nkw=parabolica&_sacat=See-All-Categories

Decodificadores (15)

Televisión Digital Terrestre (6)

Televisores (2)

Radioaficionado (1)

Informática y PDAs (4)

Redes (4)

Música, CD y Vinilos (4)

Ver todas las categorías

▼ Precio

€ ▭ a € ▭

▼ Estado

☐ Nuevo

☐ Usado

☐ Sin especificar

Elegir más...

▼ Vendedor

Especifica vendedores...

Mis preferencias

		Precio	30002	restante
Feeder Abaks 2.4Ghz para antena parabolica 24-27dbi Ubicación: España Ampliar	0 Pujas	23,00 EUR	+7,00 EUR	2d 8h 9m
KIT ANTENA PARABOLICA 60CM + LNB 0,1 dB Ubicación: España	¡Cómpralo ya!	19,99 EUR	+9,00 EUR	30d 8h 10m
ANTENA PARABOLICA SATYCON 60CM (KIT COMPLETO) Ubicación: España	¡Cómpralo ya!	20,83 EUR	+9,00 EUR	6d 2h 56m
ANTENA PARABOLICA SATYCON 80CM (KIT COMPLETO) Ubicación: España	¡Cómpralo ya!	29,16 EUR	+9,00 EUR	6d 2h 56m
LOCALIZADOR DE SATELITE PARA ANTENA PARABOLICA Muy practico y economico para localizar satelites Ubicación: España	¡Cómpralo ya!	12,00 EUR	+8,00 EUR	68d 23h 19m

¿NO ENCUENTRAS LO QUE ESTÁS BUSCANDO?

DVB Data

Linux has the modules for this card by default, we only need the tools to manage it:

linuxtv-dvb-apps

My version is 1.1.1 and I use Fedora (Not too cool to use Debian :P).

Sniffing Data

Once the antenna and the card is installed and linuxtv-dvb-apps compiled and installed, the process is:

1- Tune the DVB Card

2- Find a PID with data

3- Create an Ethernet interface associated to that PID

We can repeat 2 to 3 any times we want.

Sniffing Data

1- **Tune the DVB Card**

2- Find a PID with data

3- Create an Ethernet interface associated to that PID

Sniffing Data

Tune DVB Card

The tool we must use is *szap* and we need the transponder’s parameters in a configuration file.

For example, for “Sirius-4 Nordic Beam":

```
# echo “sirius4N:12322:v:0:27500:0:0:0" >> channels.conf
```

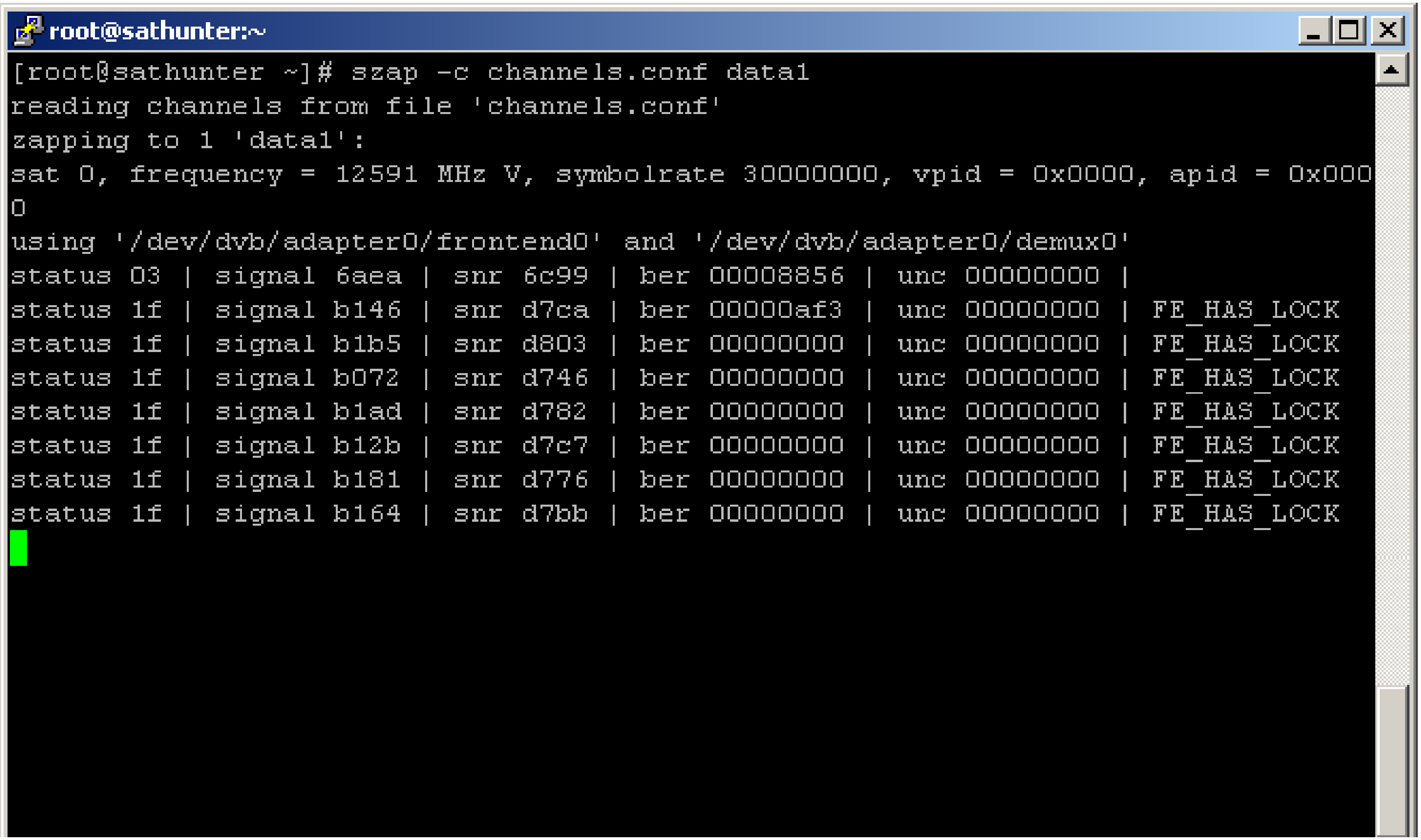
Sniffing Data

We run szap with the channel configuration file and the transponder we want use (the configuration file can have more than one).

```
# szap –c channels.conf sirius4N
```

We must keep it running.

Sniffing Data



```
[root@sathunter ~]# szap -c channels.conf data1
reading channels from file 'channels.conf'
zapping to 1 'data1':
sat 0, frequency = 12591 MHz V, symbolrate 30000000, vpid = 0x0000, apid = 0x000
0
using '/dev/dvb/adapter0/frontend0' and '/dev/dvb/adapter0/demux0'
status 03 | signal 6aea | snr 6c99 | ber 00008856 | unc 00000000 |
status 1f | signal b146 | snr d7ca | ber 00000af3 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b1b5 | snr d803 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b072 | snr d746 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b1ad | snr d782 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b12b | snr d7c7 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b181 | snr d776 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b164 | snr d7bb | ber 00000000 | unc 00000000 | FE_HAS_LOCK
```

Sniffing Data

The transponder parameters can be found around Internet.

http://www.fastsatfinder.com/transponders.html

Sniffing Data

1- Tune the DVB Card

2- **Find a PID with data**

3- Create an Ethernet interface associated to that PID

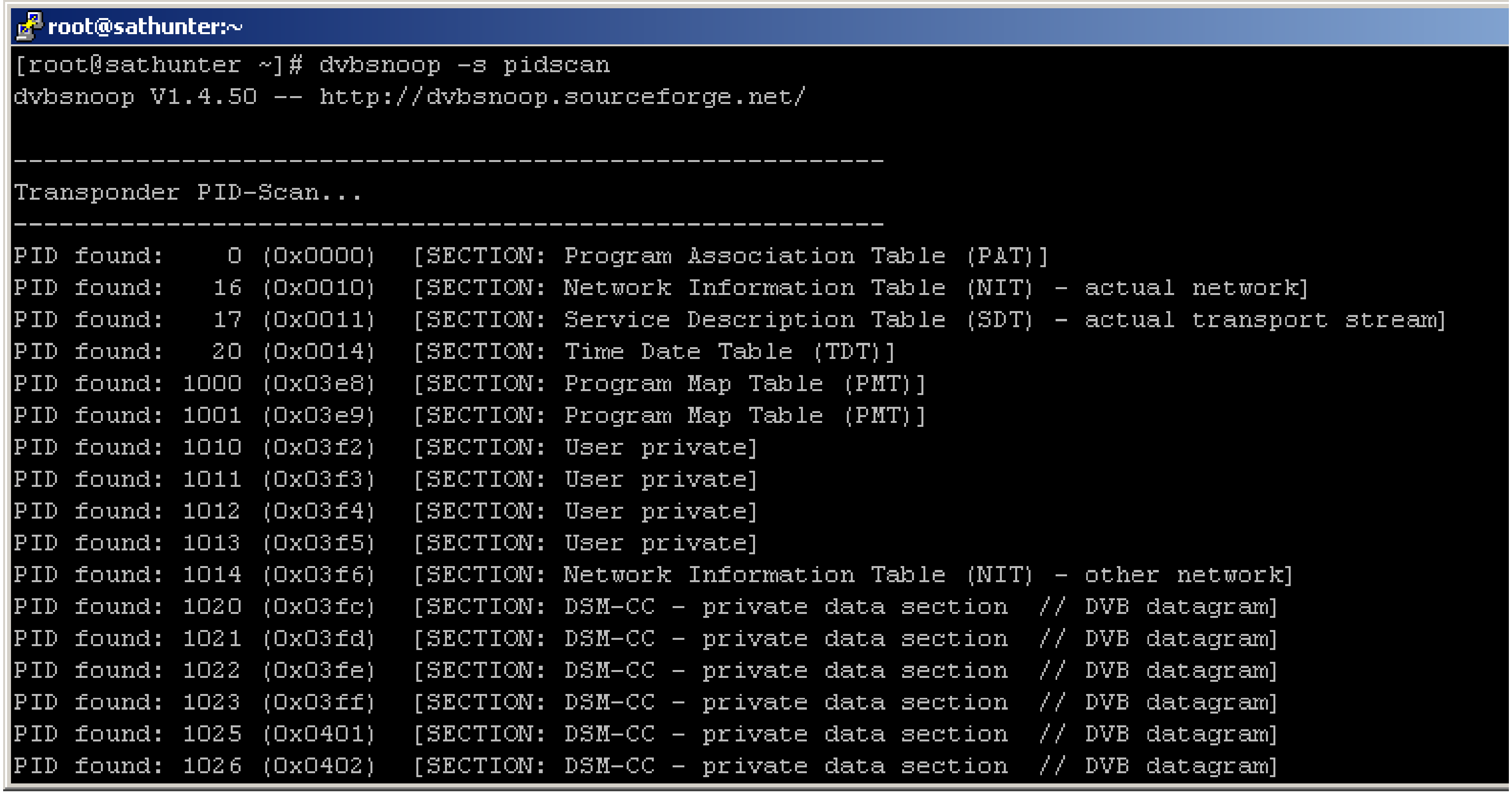
Sniffing Data

- Find a PID

```
#dvbsnoop -s pidscan
```

Search for *data section* on results.

Sniffing Data



```
[root@sathunter ~]# dvbsnoop -s pidscan
dvbsnoop V1.4.50 -- 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:   20 (0x0014)  [SECTION: Time Date Table (TDT)]
PID found: 1000 (0x03e8)  [SECTION: Program Map Table (PMT)]
PID found: 1001 (0x03e9)  [SECTION: Program Map Table (PMT)]
PID found: 1010 (0x03f2)  [SECTION: User private]
PID found: 1011 (0x03f3)  [SECTION: User private]
PID found: 1012 (0x03f4)  [SECTION: User private]
PID found: 1013 (0x03f5)  [SECTION: User private]
PID found: 1014 (0x03f6)  [SECTION: Network Information Table (NIT) - other network]
PID found: 1020 (0x03fc)  [SECTION: DSM-CC - private data section  // DVB datagram]
PID found: 1021 (0x03fd)  [SECTION: DSM-CC - private data section  // DVB datagram]
PID found: 1022 (0x03fe)  [SECTION: DSM-CC - private data section  // DVB datagram]
PID found: 1023 (0x03ff)  [SECTION: DSM-CC - private data section  // DVB datagram]
PID found: 1025 (0x0401)  [SECTION: DSM-CC - private data section  // DVB datagram]
PID found: 1026 (0x0402)  [SECTION: DSM-CC - private data section  // DVB datagram]
```

Sniffing Data

1- Tune the DVB Card

2- Find a PID with data

3- **Create an Ethernet interface associated to that PID**

Sniffing Data

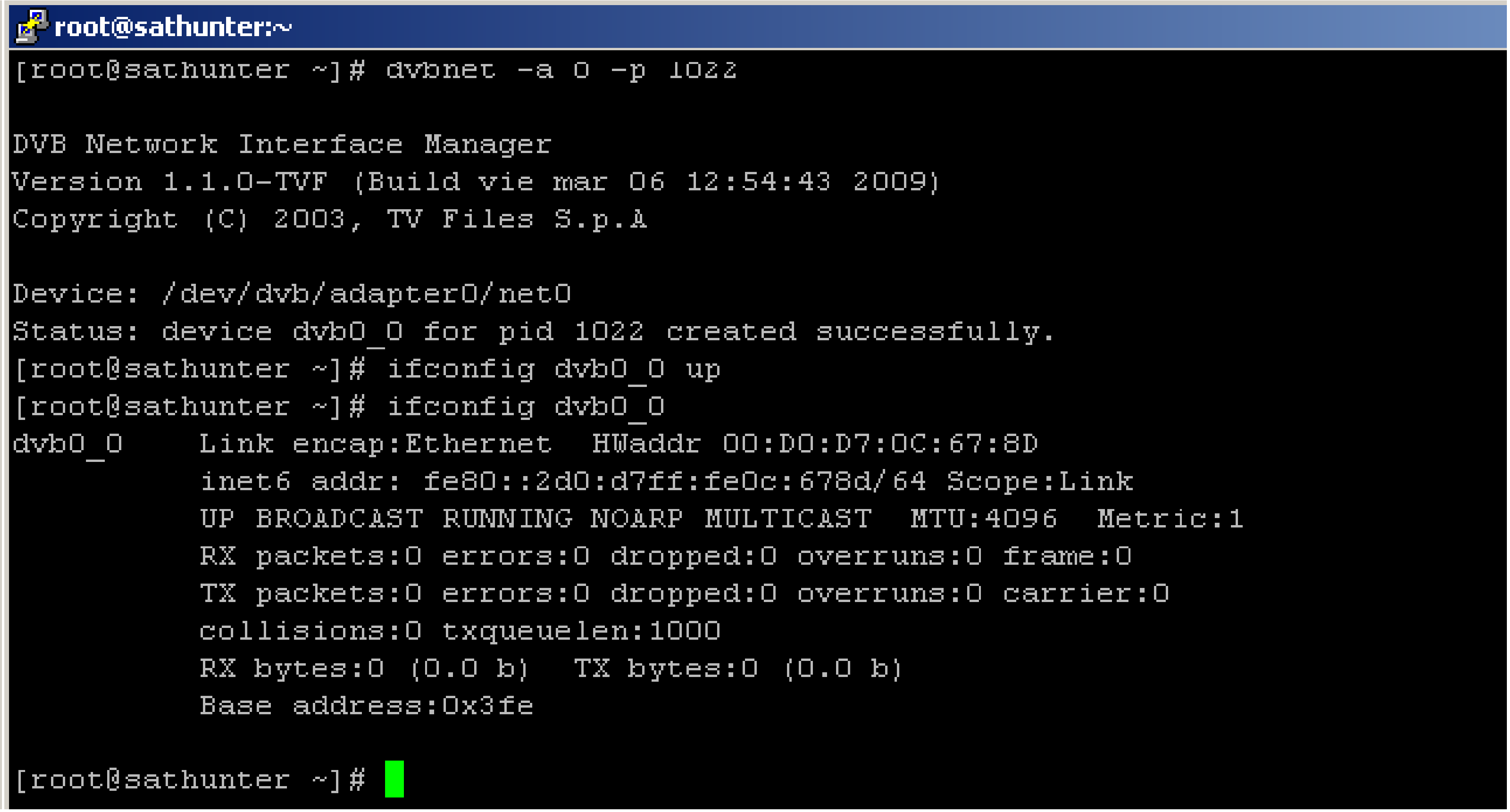
- Create an interface associated to a PID

```
#dvbnet -a <adapter number> -p <PID>
```

- Activate it

```
#ifconfig dvb0_<iface number> up
```

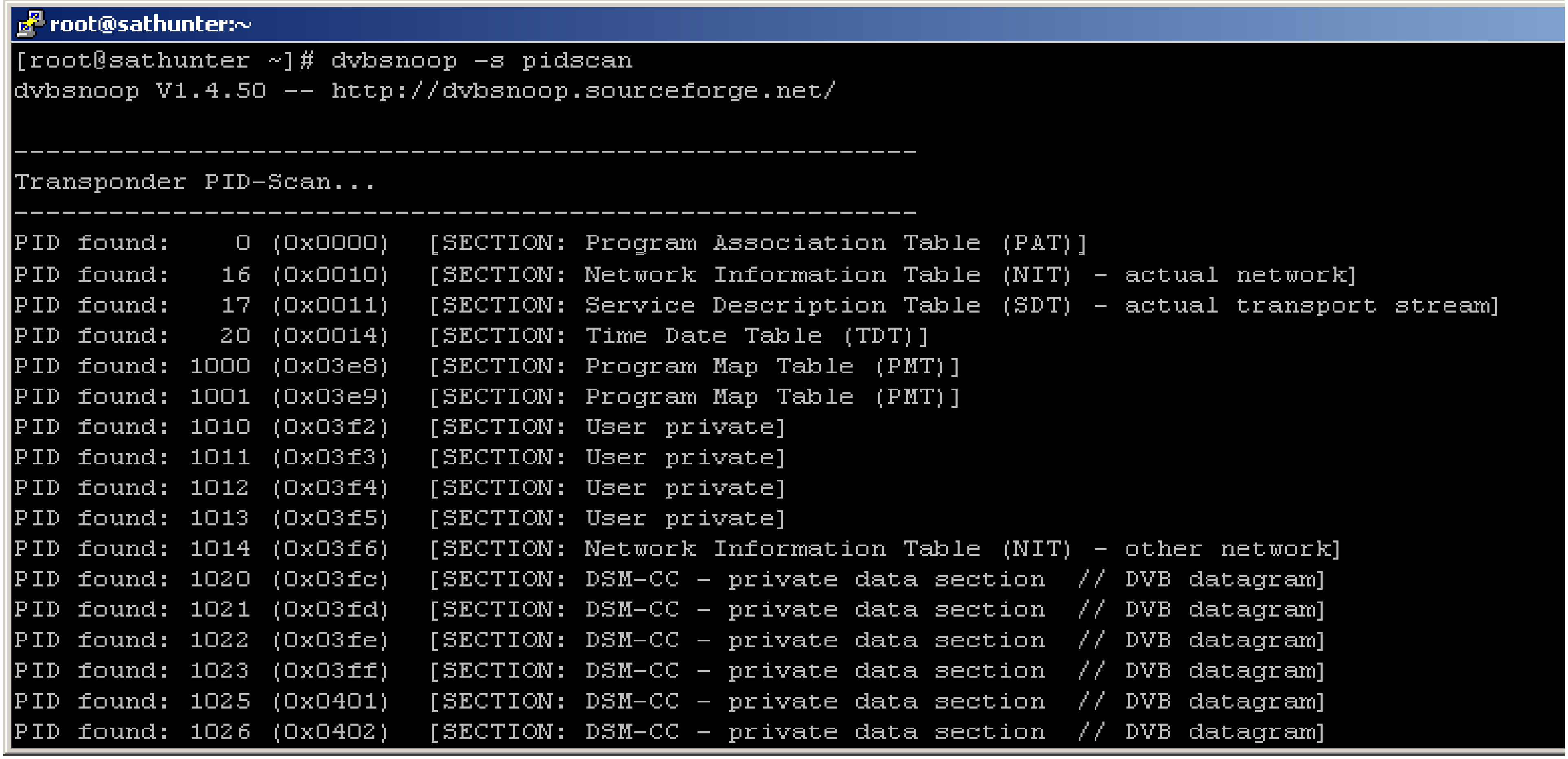
Sniffing Data



```
[root@sathunter ~]# dvbnet -a 0 -p 1022

DVB Network Interface Manager
Version 1.1.0-TVF (Build vie mar 06 12:54:43 2009)
Copyright (C) 2003, TV Files S.p.A

Device: /dev/dvb/adapter0/net0
Status: device dvb0_0 for pid 1022 created successfully.
[root@sathunter ~]# ifconfig dvb0_0 up
[root@sathunter ~]# ifconfig dvb0_0
dvb0_0    Link encap:Ethernet  HWaddr 00:D0:D7:0C:67:8D
          inet6 addr: fe80::2d0:d7ff:fe0c:678d/64 Scope:Link
          UP BROADCAST RUNNING 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:0x3fe

[root@sathunter ~]# 
```

Sniffing Data

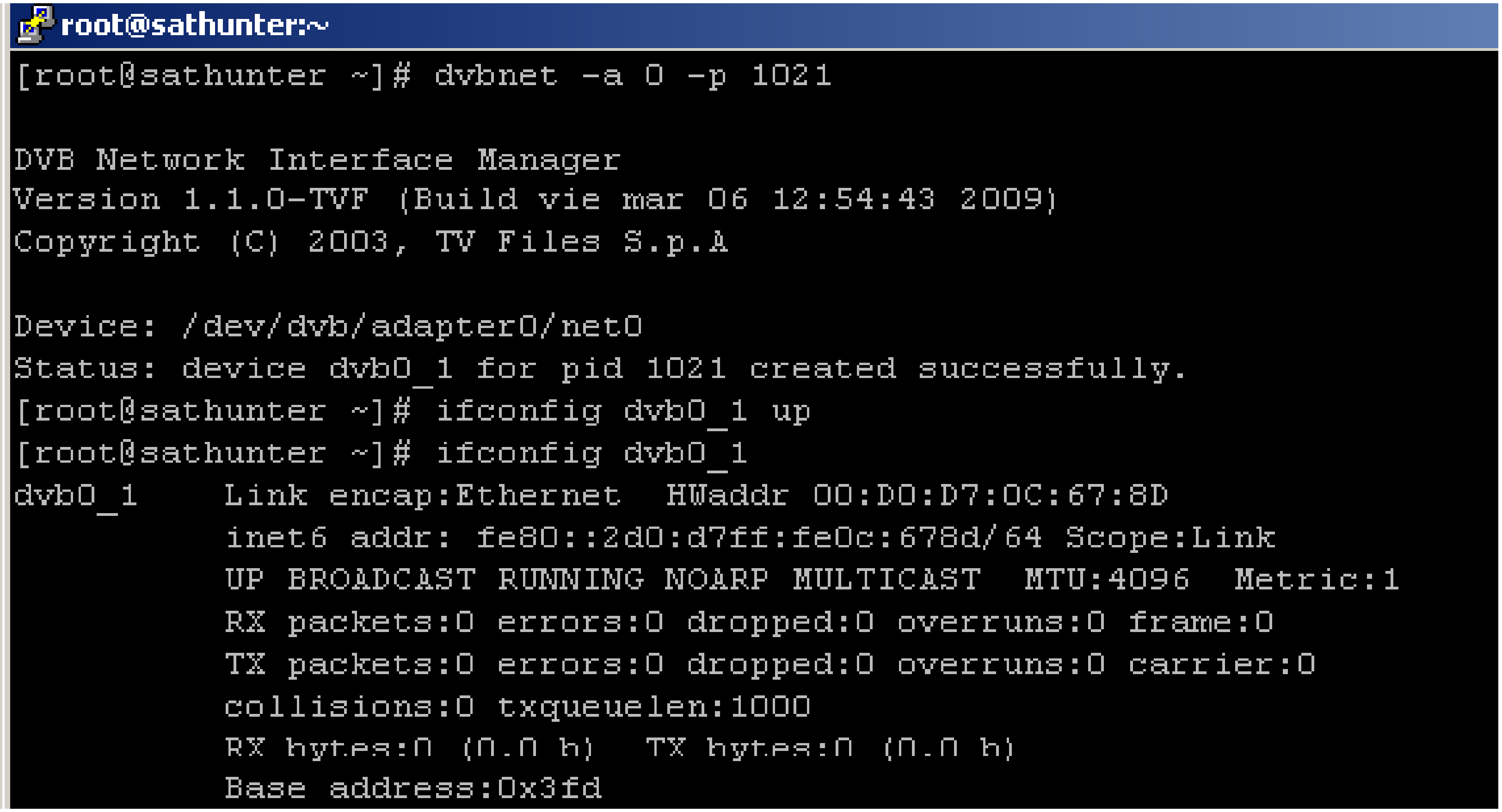
Back to de pidscan results



```
[root@sathunter ~]# dvbsnoop -s pidscan
dvbsnoop V1.4.50 -- 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:   20 (0x0014)  [SECTION: Time Date Table (TDT)]
PID found: 1000 (0x03e8)  [SECTION: Program Map Table (PMT)]
PID found: 1001 (0x03e9)  [SECTION: Program Map Table (PMT)]
PID found: 1010 (0x03f2)  [SECTION: User private]
PID found: 1011 (0x03f3)  [SECTION: User private]
PID found: 1012 (0x03f4)  [SECTION: User private]
PID found: 1013 (0x03f5)  [SECTION: User private]
PID found: 1014 (0x03f6)  [SECTION: Network Information Table (NIT) - other network]
PID found: 1020 (0x03fc)  [SECTION: DSM-CC - private data section  // DVB datagram]
PID found: 1021 (0x03fd)  [SECTION: DSM-CC - private data section  // DVB datagram]
PID found: 1022 (0x03fe)  [SECTION: DSM-CC - private data section  // DVB datagram]
PID found: 1023 (0x03ff)  [SECTION: DSM-CC - private data section  // DVB datagram]
PID found: 1025 (0x0401)  [SECTION: DSM-CC - private data section  // DVB datagram]
PID found: 1026 (0x0402)  [SECTION: DSM-CC - private data section  // DVB datagram]
```

Sniffing Data

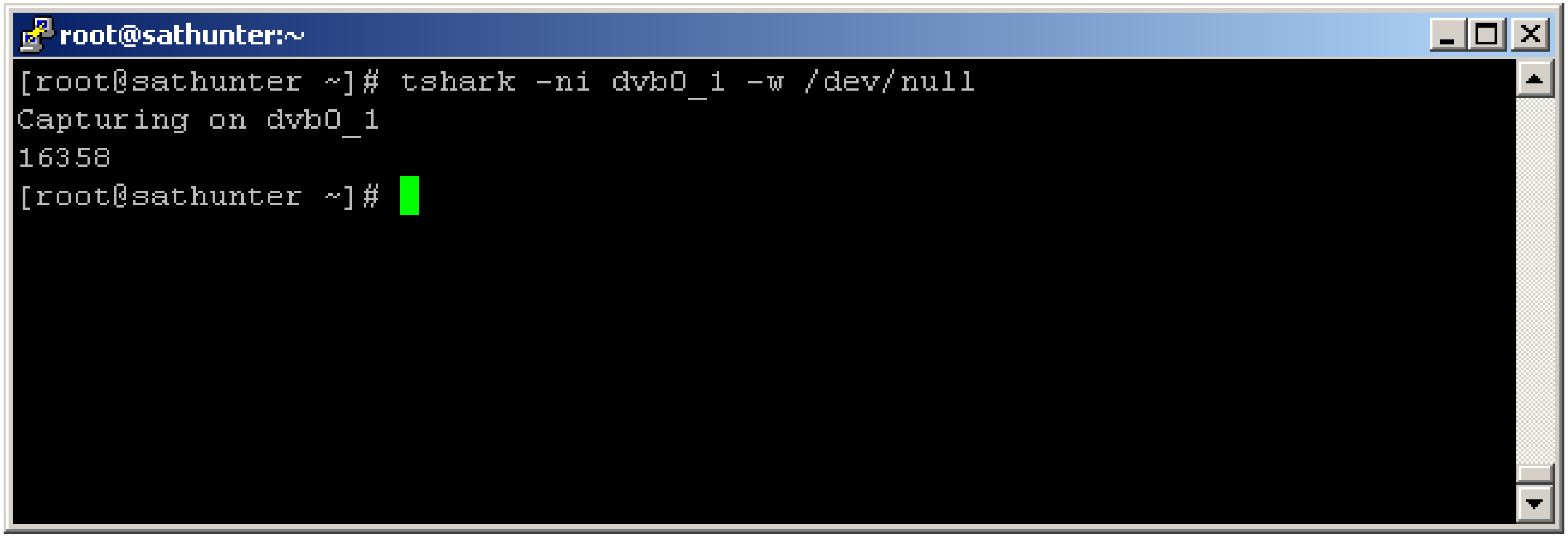
Create another interface



```
[root@sathunter ~]# dvbnet -a 0 -p 1021

DVB Network Interface Manager
Version 1.1.0-TVF (Build vie mar 06 12:54:43 2009)
Copyright (C) 2003, TV Files S.p.A

Device: /dev/dvb/adapter0/net0
Status: device dvb0_1 for pid 1021 created successfully.
[root@sathunter ~]# ifconfig dvb0_1 up
[root@sathunter ~]# ifconfig dvb0_1
dvb0_1    Link encap:Ethernet  HWaddr 00:D0:D7:0C:67:8D
          inet6 addr: fe80::2d0:d7ff:fe0c:678d/64 Scope:Link
          UP BROADCAST RUNNING 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:0x3fd
```

Sniffing Data

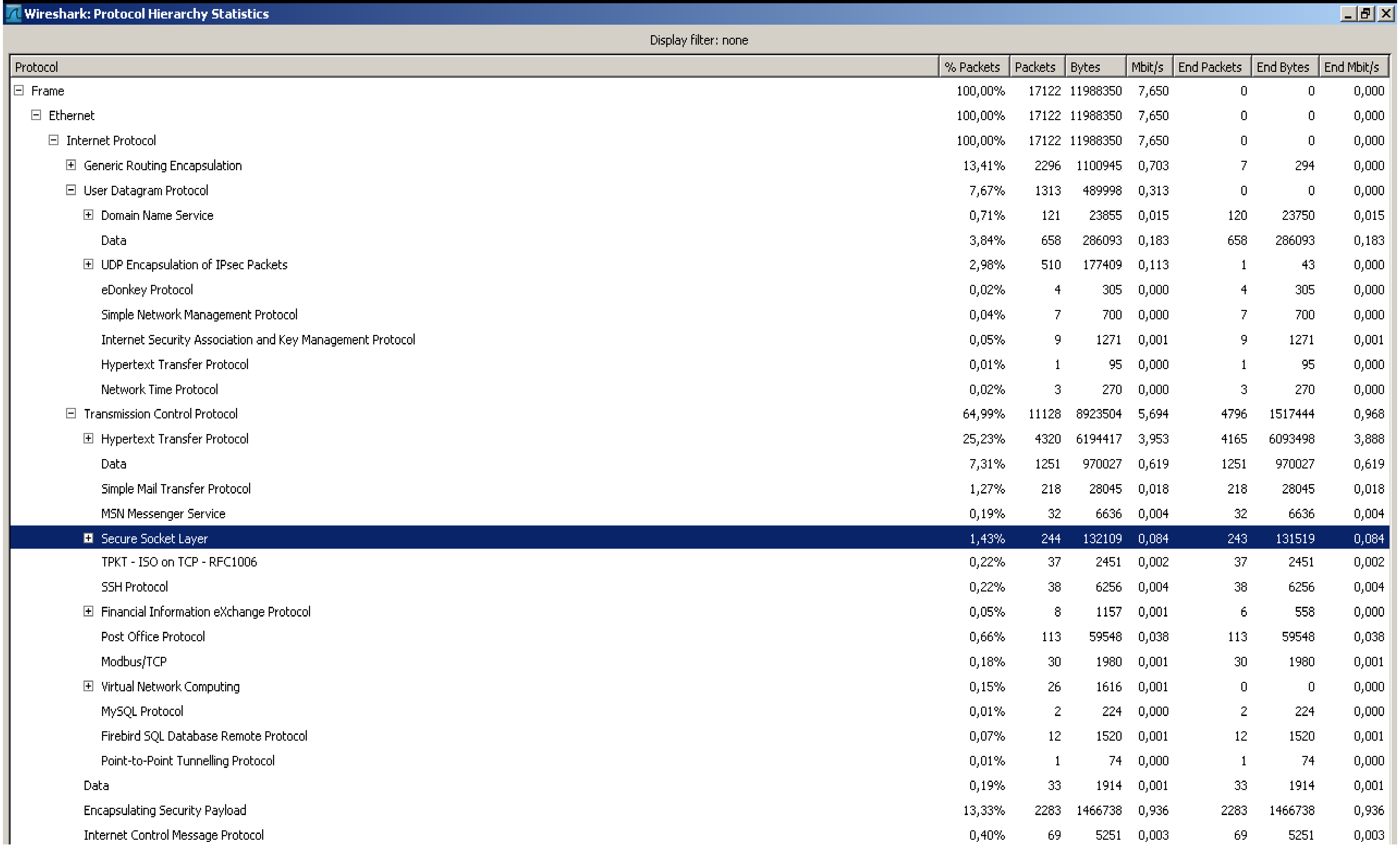
Wireshark is our friend



```
[root@sathunter ~]# tshark -ni dvb0_1 -w /dev/null
Capturing on dvb0_1
16358
[root@sathunter ~]#
```

16358 packets in 10 seconds

Sniffing data



Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
⊟ Frame	100,00%	17122	11988350	7,650	0	0	0,000
⊟ Ethernet	100,00%	17122	11988350	7,650	0	0	0,000
⊟ Internet Protocol	100,00%	17122	11988350	7,650	0	0	0,000
⊞ Generic Routing Encapsulation	13,41%	2296	1100945	0,703	7	294	0,000
⊟ User Datagram Protocol	7,67%	1313	489998	0,313	0	0	0,000
⊞ Domain Name Service	0,71%	121	23855	0,015	120	23750	0,015
Data	3,84%	658	286093	0,183	658	286093	0,183
⊞ UDP Encapsulation of IPsec Packets	2,98%	510	177409	0,113	1	43	0,000
eDonkey Protocol	0,02%	4	305	0,000	4	305	0,000
Simple Network Management Protocol	0,04%	7	700	0,000	7	700	0,000
Internet Security Association and Key Management Protocol	0,05%	9	1271	0,001	9	1271	0,001
Hypertext Transfer Protocol	0,01%	1	95	0,000	1	95	0,000
Network Time Protocol	0,02%	3	270	0,000	3	270	0,000
⊟ Transmission Control Protocol	64,99%	11128	8923504	5,694	4796	1517444	0,968
⊞ Hypertext Transfer Protocol	25,23%	4320	6194417	3,953	4165	6093498	3,888
Data	7,31%	1251	970027	0,619	1251	970027	0,619
Simple Mail Transfer Protocol	1,27%	218	28045	0,018	218	28045	0,018
MSN Messenger Service	0,19%	32	6636	0,004	32	6636	0,004
⊞ Secure Socket Layer	1,43%	244	132109	0,084	243	131519	0,084
TPKT - ISO on TCP - RFC1006	0,22%	37	2451	0,002	37	2451	0,002
SSH Protocol	0,22%	38	6256	0,004	38	6256	0,004
⊞ Financial Information eXchange Protocol	0,05%	8	1157	0,001	6	558	0,000
Post Office Protocol	0,66%	113	59548	0,038	113	59548	0,038
Modbus/TCP	0,18%	30	1980	0,001	30	1980	0,001
⊞ Virtual Network Computing	0,15%	26	1616	0,001	0	0	0,000
MySQL Protocol	0,01%	2	224	0,000	2	224	0,000
Firebird SQL Database Remote Protocol	0,07%	12	1520	0,001	12	1520	0,001
Point-to-Point Tunnelling Protocol	0,01%	1	74	0,000	1	74	0,000
Data	0,19%	33	1914	0,001	33	1914	0,001
Encapsulating Security Payload	13,33%	2283	1466738	0,936	2283	1466738	0,936
Internet Control Message Protocol	0,40%	69	5251	0,003	69	5251	0,003

Sniffing Data

- We can have more than one PID assigned to an interface, this will be very useful.
- Malicious users can:
  - Catch passwords.
  - Catch cookies and get into authenticated HTTP sessions.
  - Read emails
  - Catch sensitive files
  - Do traffic analysis
  - Etc ….

Sniffing Data

Reminder:

In satellite communications we have two scenarios:

A- Satmodem, Only Downlink via Satellite

B- Astromodem, Both uplink and downlink via Satellite.

Sniffing Data

We can only sniff the downloaded data. We can only sniff one direction in a connection.

Some "old" Stuff in Sat hacking

- DNS Spoofing
- TCP hijacking
- Attacking GRE

DNS Spoofing

DNS Spoofing is the art of making a DNS entry to point to an another IP than it would be supposed to point to. (SecureSphere)

DNS Spoofing

- Data we need to perform this attack
  - DNS Request ID
  - Source Port
  - Source IP
  - Destination IP
  - Name/IP asking for

DNS Spoofing

- It´s trivial to see that if we sniff a DNS request we have all that information and we can spoof the answer.

- Many tools around do this job, the only thing we also need is to be faster than the real DNS server (jizz).

DNS Spoofing

- Why is this attack important?
  - Think in phising
  - With this attack, uplink sniff can be possible
    - Rogue WPAD service
    - Sslstrip can be use to avoid SSL connections.

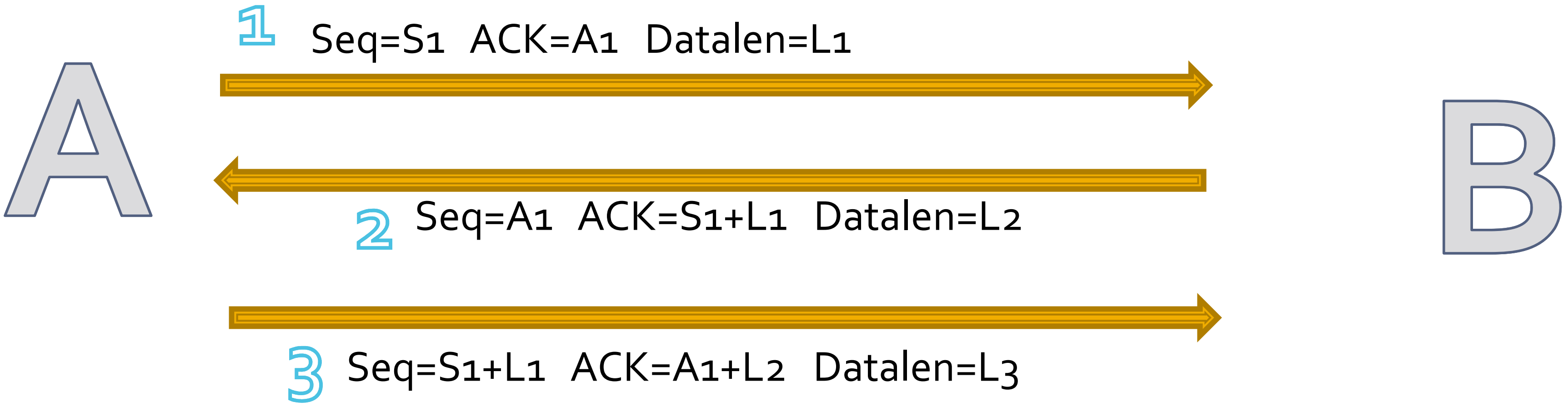
Some “old” Stuff in Sat hacking

- DNS Spoofing
- TCP hijacking
- Attacking GRE

TCP hijacking

TCP session **hijacking** is when a hacker takes over a **TCP** session between two machines. (ISS)

TCP hijacking



A

B

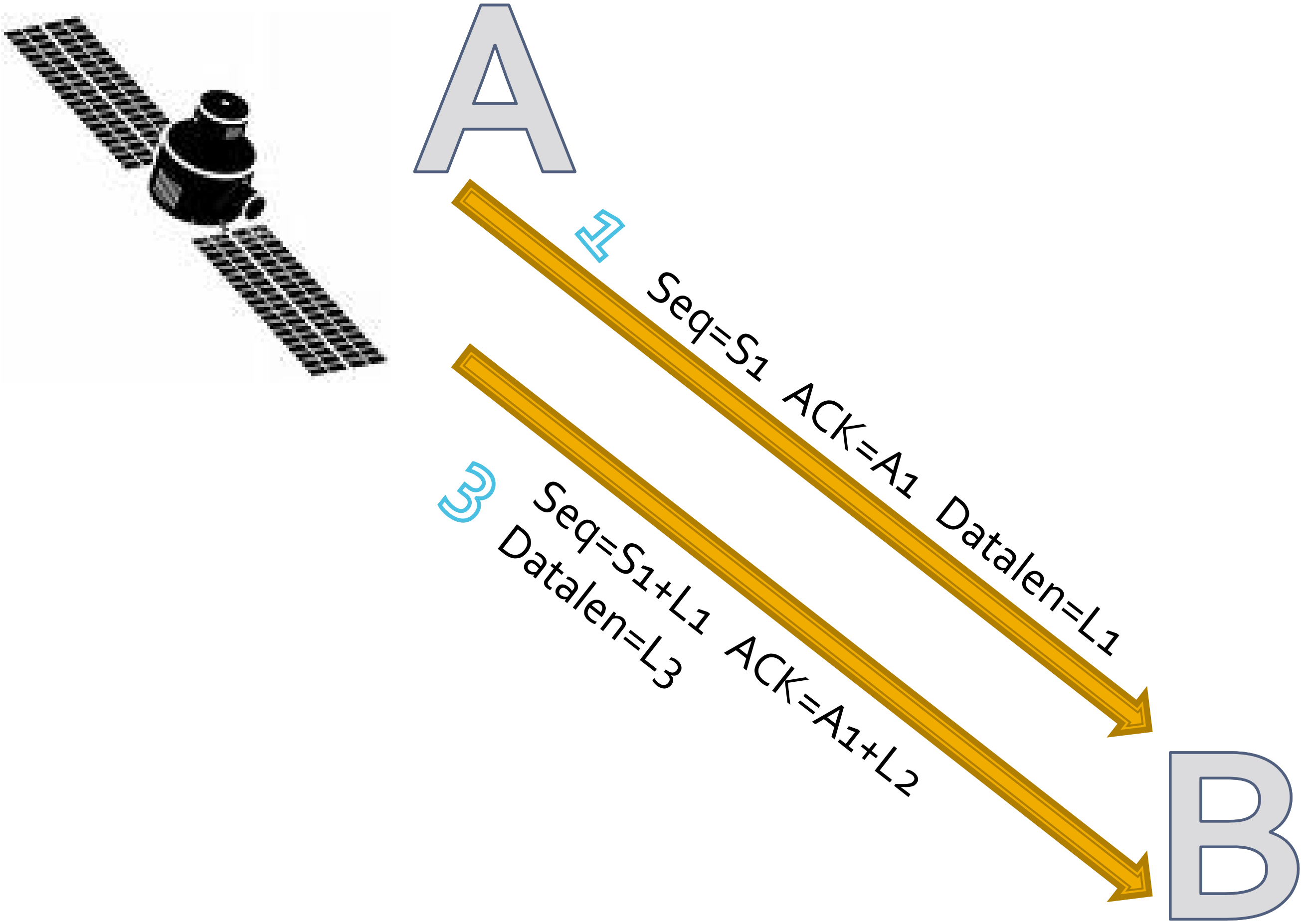
1 Seq=S1 ACK=A1 Datalen=L1

2 Seq=A1 ACK=S1+L1 Datalen=L2

3 Seq=S1+L1 ACK=A1+L2 Datalen=L3

If we sniff 1 we can predict Seq and Ack of 2 and we can send the payload we want in 2

TCP Hijacking



A

1 Seq=S1 ACK=A1 Datalen=L1

3 Seq=S1+L1 ACK=A1+L2
Datalen=L3

B

TCP Hijacking

- Initially we can only have a false connection with A.

- In certain circumstances, we can make this attack with B, when L2 is predictable.

- Some tools for doing this:
  - Hunt
  - Shijack
  - Scapy

Some “old” Stuff in Sat hacking

- DNS Spoofing
- TCP hijacking
- Attacking GRE

Attacking GRE

- Generic Routing Encapsulation

- Point to point tunneling protocol

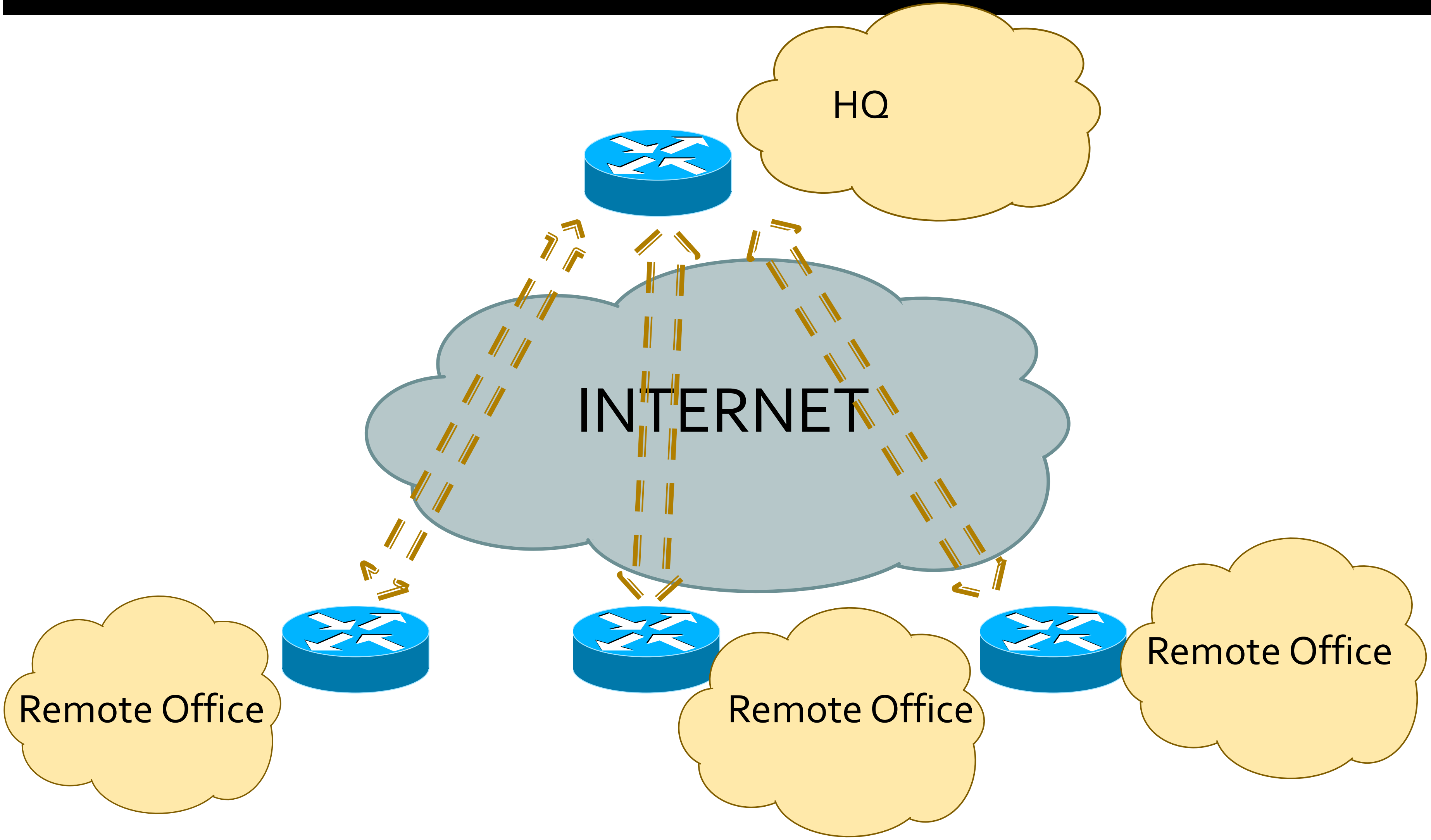
- 13% of Satellite’s data traffic in our transponder is GRE

Attacking GRE

This chapter is based in Phenoelit's discussion paper written by FX applied to satellite scenario.

Original paper:
http://www.phenoelit-us.org/irpas/gre.html

Attacking GRE



Attacking GRE

Find a target:

```
#tshark –ni dvbo_o –R gre –w capture.cap
```

Attacking GRE

GRE Packet

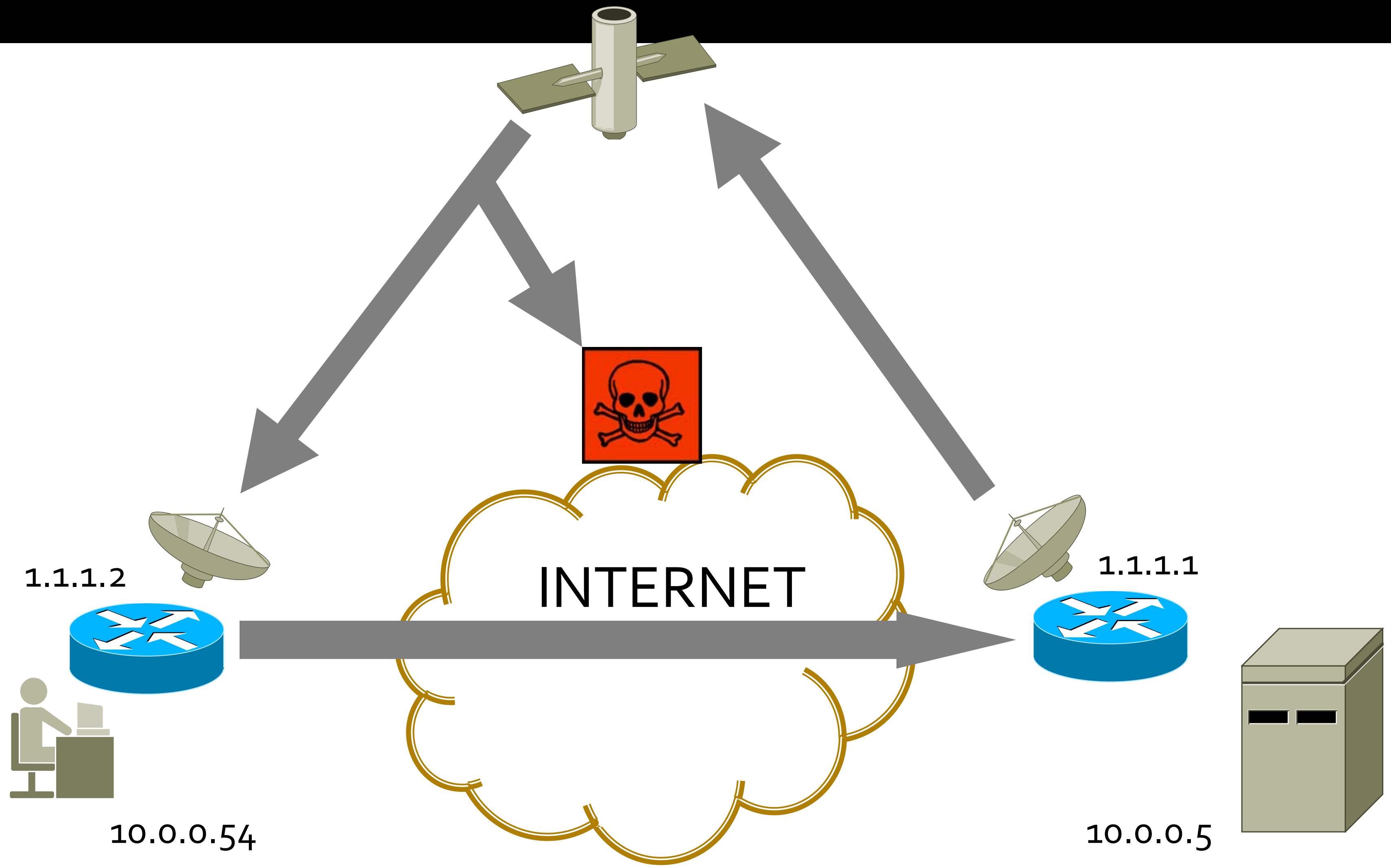
IP dest 1	**IP source 1**
GRE header	
Payload IP dest	Payload IP source
Payload IP Header	
Payload Data	

Attacking GRE

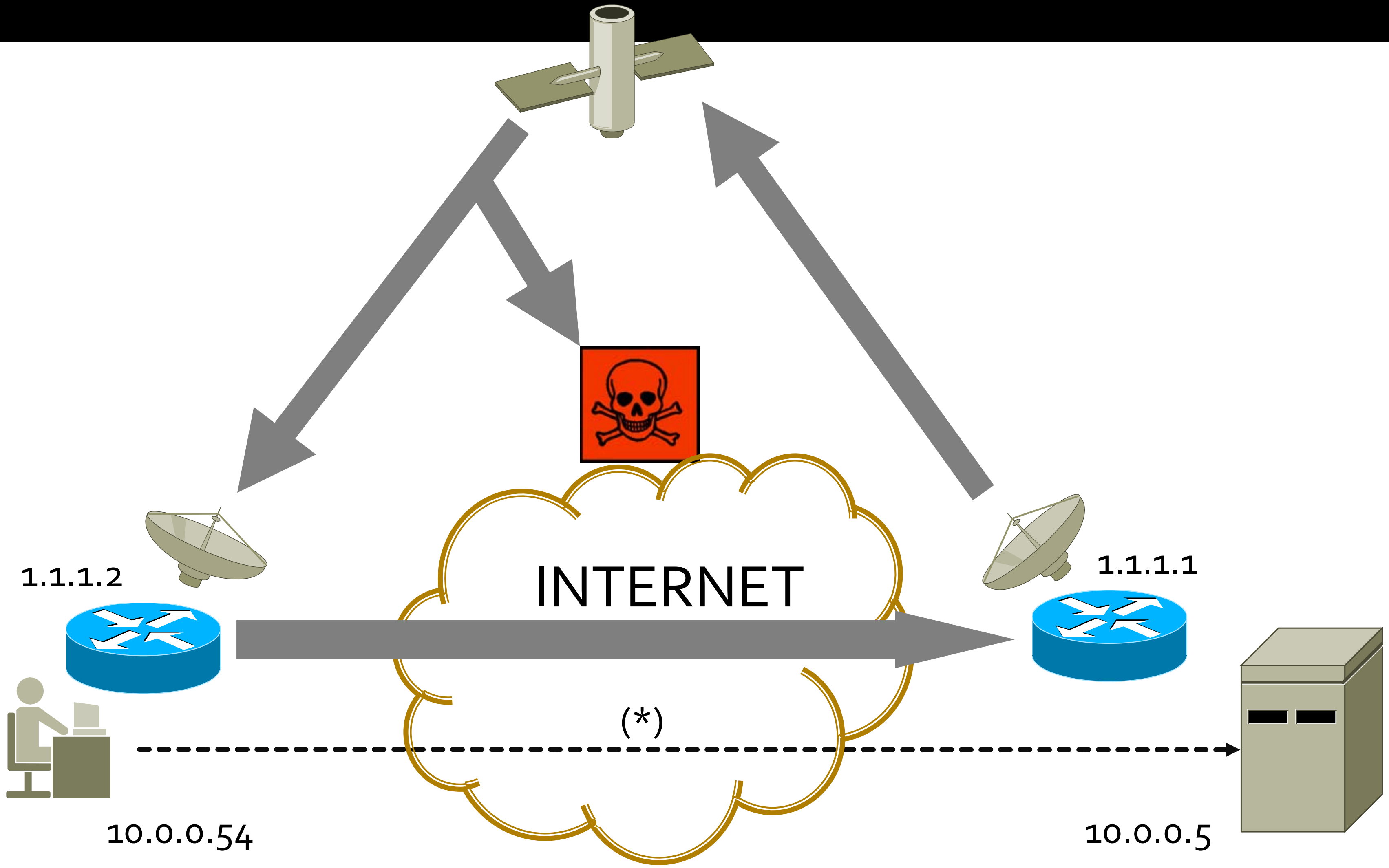
- IP dest 1 and source 1 must be Internet reachable IPs

- The payload´s IPs used to be internal.

Attacking GRE



Attacking GRE

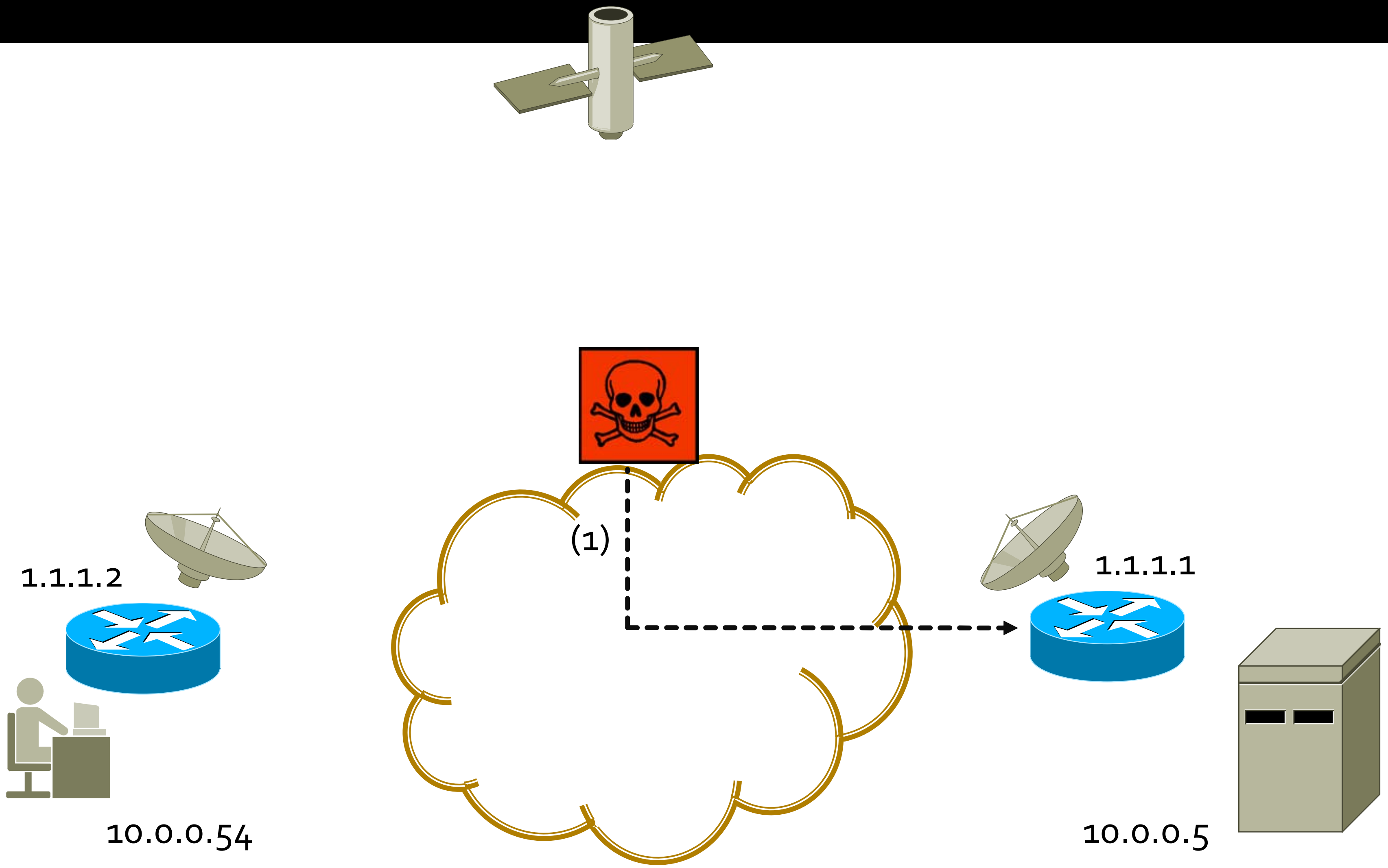


Attacking GRE

(*) GRE Packet

<table>
<tr><td><b>1.1.1.1</b></td><td><b>1.1.1.2</b></td></tr>
<tr><td colspan="2">GRE header (32 bits without flags)</td></tr>
<tr><td>10.0.0.5</td><td>10.0.0.54</td></tr>
<tr><td colspan="2">Payload IP Header</td></tr>
<tr><td colspan="2">Payload Data</td></tr>
</table>

Attacking GRE

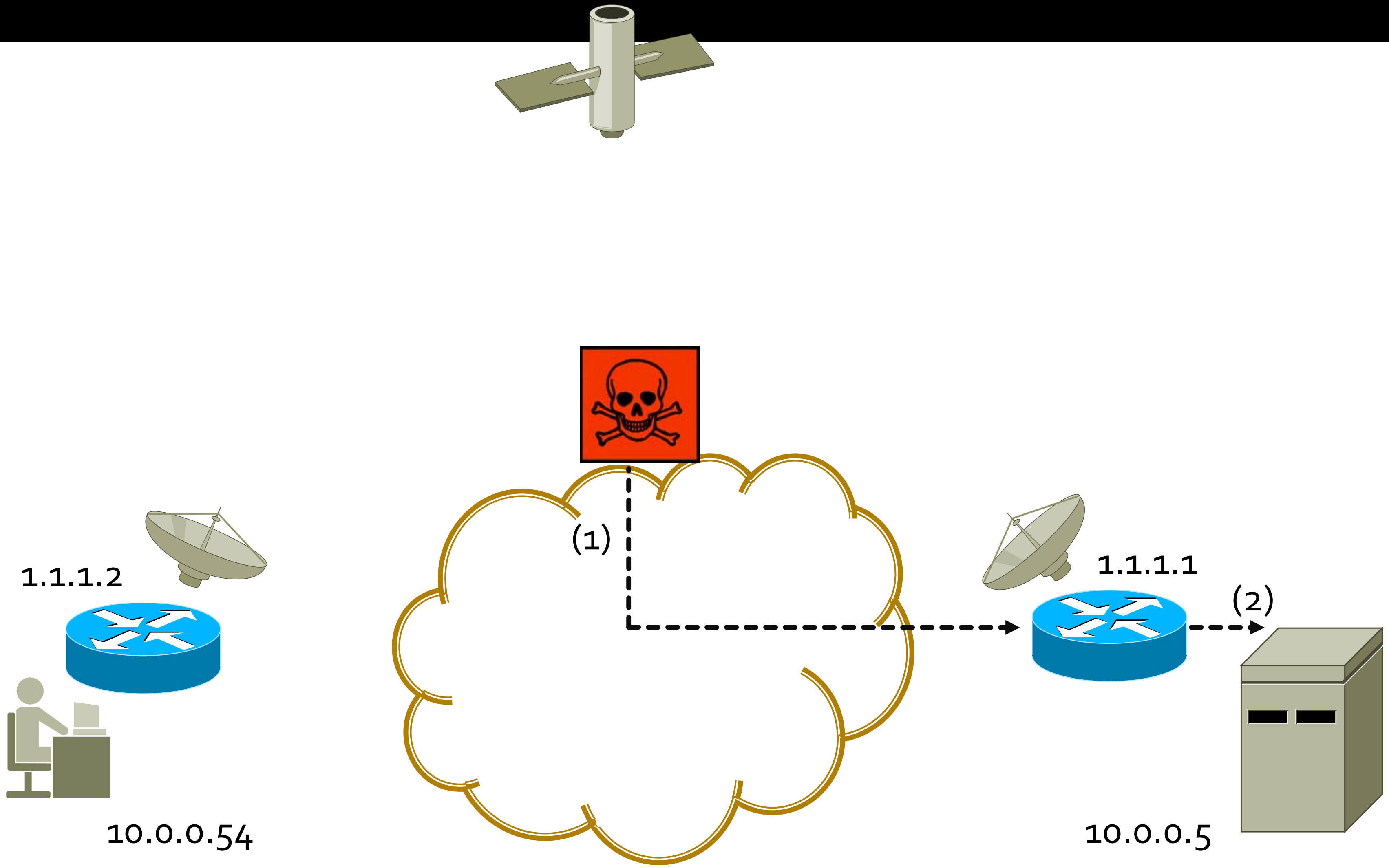


Attacking GRE

(1) GRE Packet

1.1.1.1	**1.1.1.2**
GRE header (32 bits without flags)	
10.0.0.5	10.0.0.54
Payload IP Header	
Payload Data	

Attacking GRE

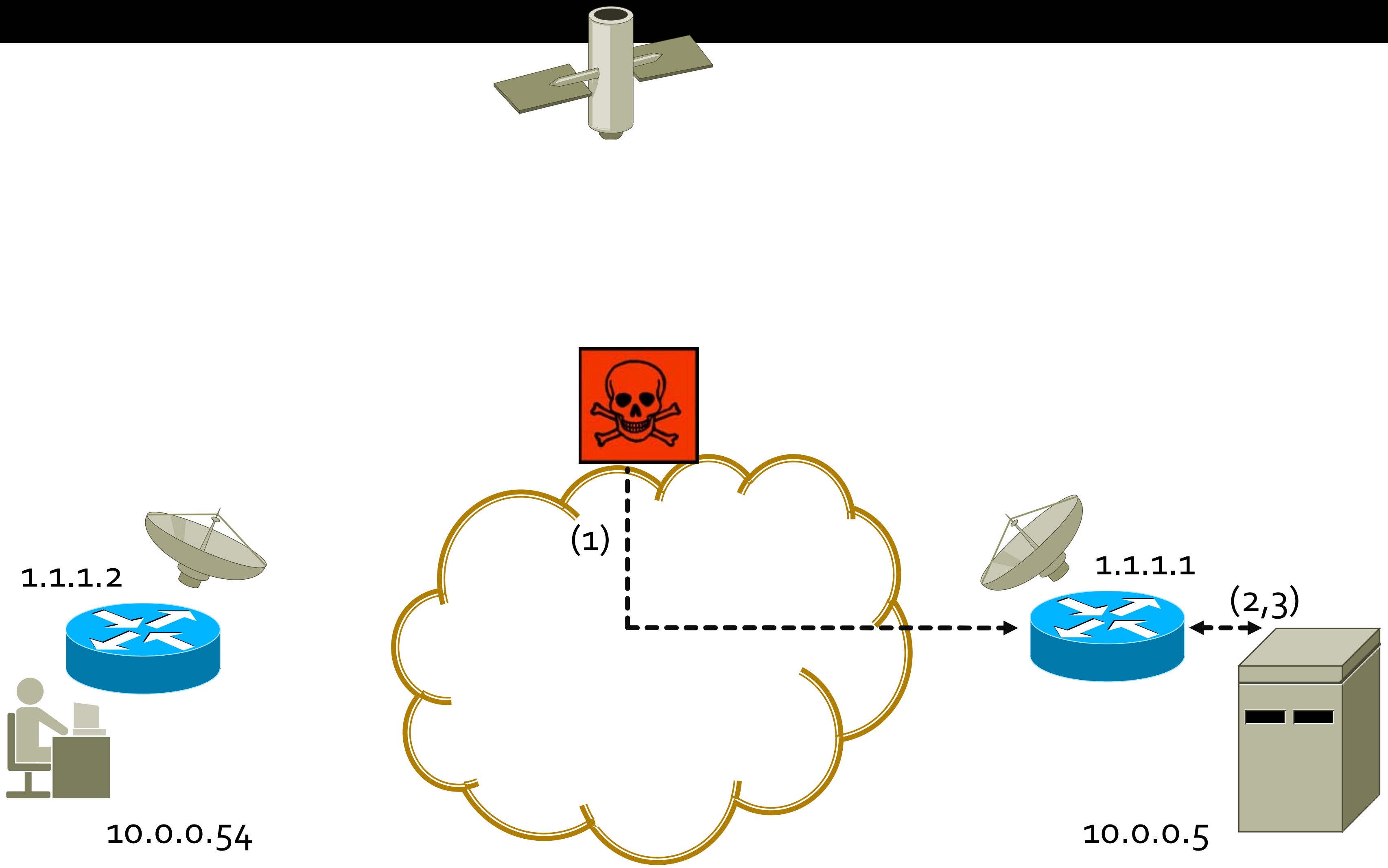


Attacking GRE

(2) IP Packet

10.0.0.5	10.0.0.54
IP header	
Data	

Attacking GRE

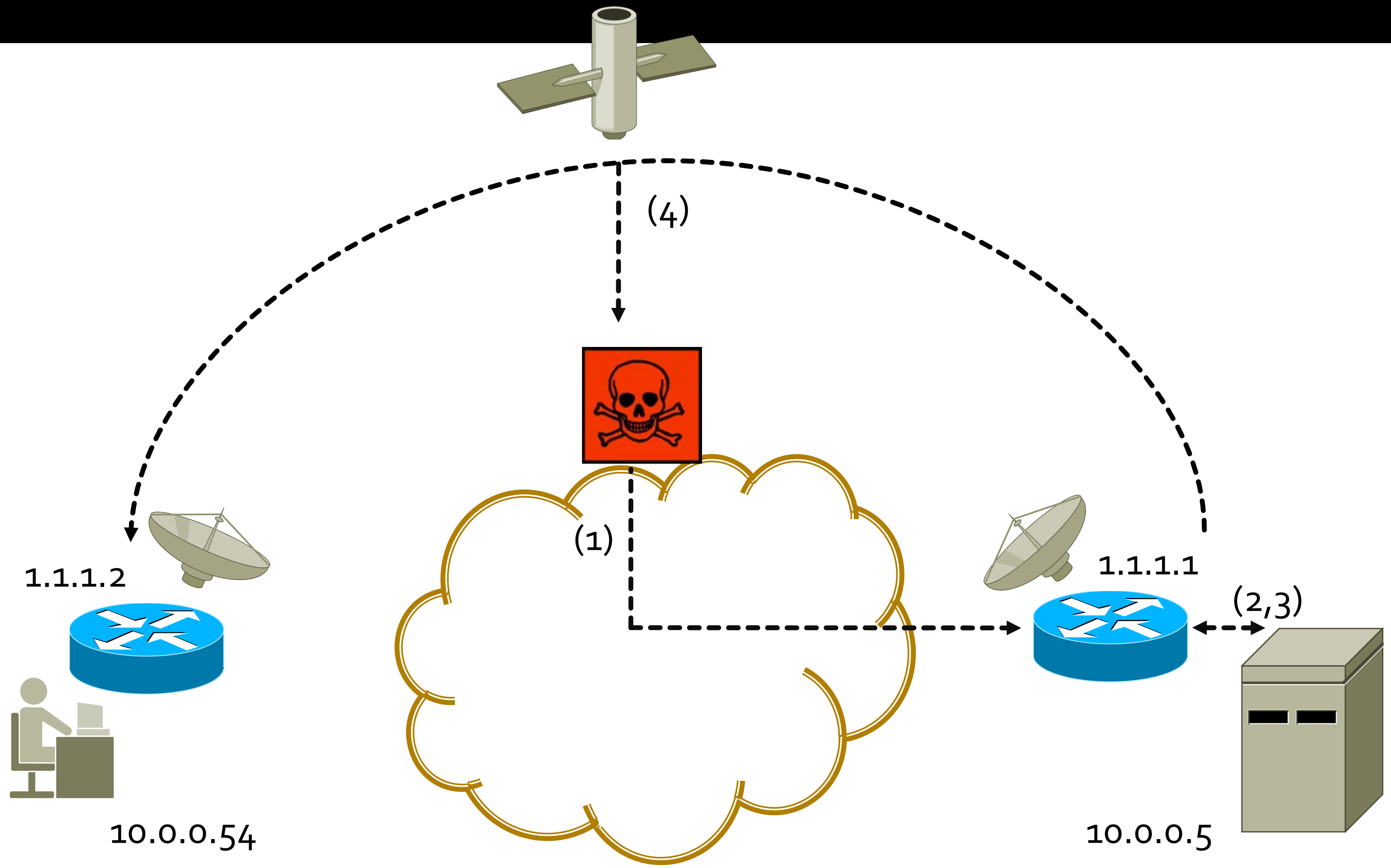


Attacking GRE

(3) IP Packet

10.0.0.54	10.0.0.5
IP header 2	
Data 2	

Attacking GRE



Attacking GRE

(4) GRE Packet

1.1.1.2	**1.1.1.1**
GRE header (32 bits without flags)	
10.0.0.54	10.0.0.5
Payload IP Header 2	
Payload Data 2	

Attacking GRE

At Phenoelit´s attack payload's IP source is our public IP. This attack lacks when that IP isn´t reachable from the internal LAN and you can be logged.

I use internal IP because we can sniff the responses.

To better improve the attack, find a internal IP not used.

HTSNACBT Attack

How
To
Scan
NSA
And
Cannot
Be
Traced

HTSNACBT Attack

We can send a *SYN packet* with any destination IP and *TCP* port (spoofing a satellite’s routable source IP) , and we can sniff the responses.

We can analyze the responses.

HTSNACBT Attack

OR… We can configure our linux like a satellite connected host.

VERY EASY!!!

HTSNACBT Attack

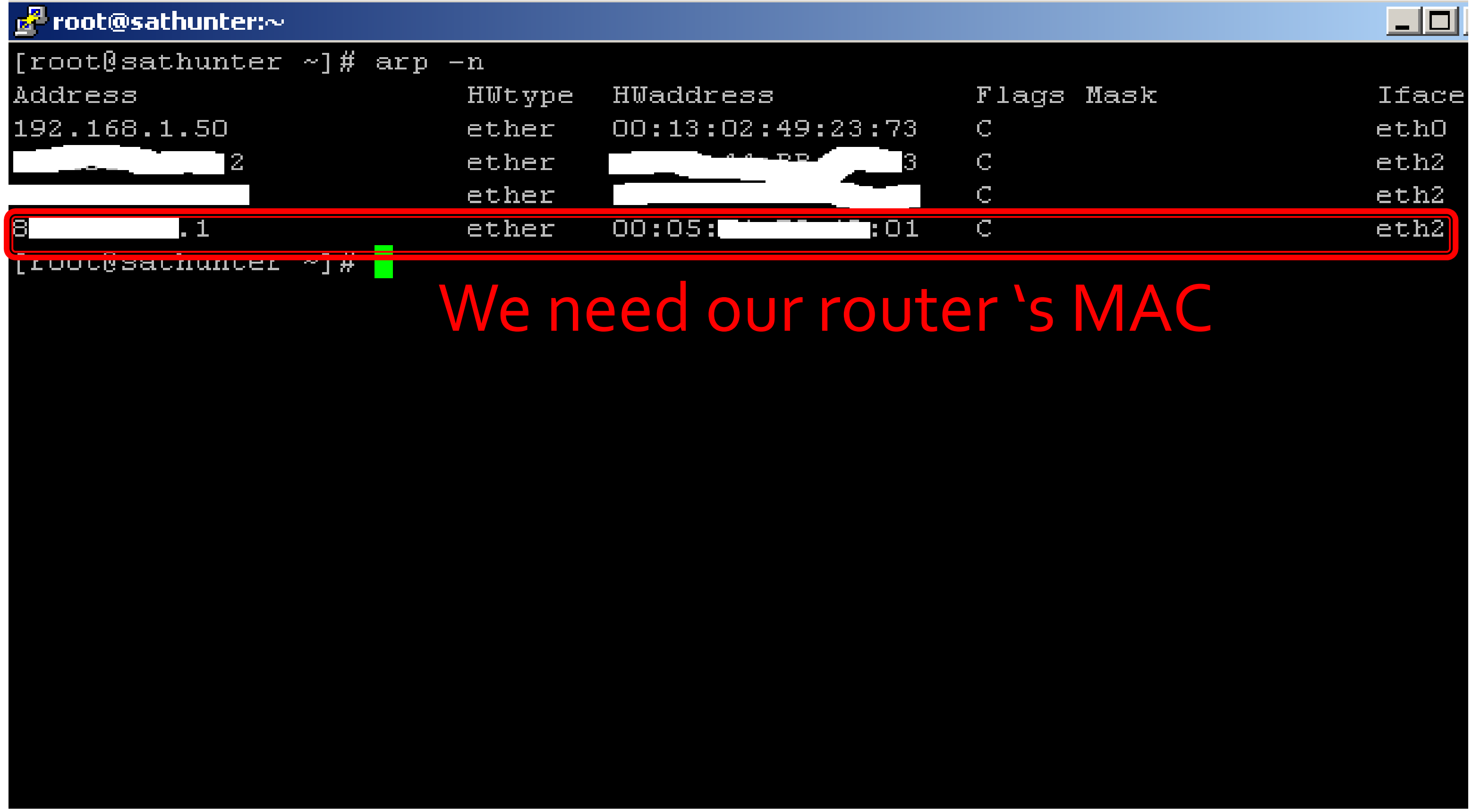
- What we need:
  - An internet connection (Let’s use it as uplink) with any technology which let you spoofing.
  - A receiver, a card….

HTSNACBT Attack

- Let’s rock!
  - Find a satellite IP not used, I ping IPs next to another sniffable satellite IP to find a non responding IP. We must sniff our ping with the DVB Card (you must save the packets).
  - This will be our IP!

HTSNACBT Attack

- Configure Linux to use it.



```
[root@sathunter ~]# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.50             ether   00:13:02:49:23:73   C                     eth0
[redacted]2              ether   [redacted]3         C                     eth2
[redacted]               ether   [redacted]          C                     eth2
8[redacted].1            ether   00:05:[redacted]:01 C                     eth2
[root@sathunter ~]#
```

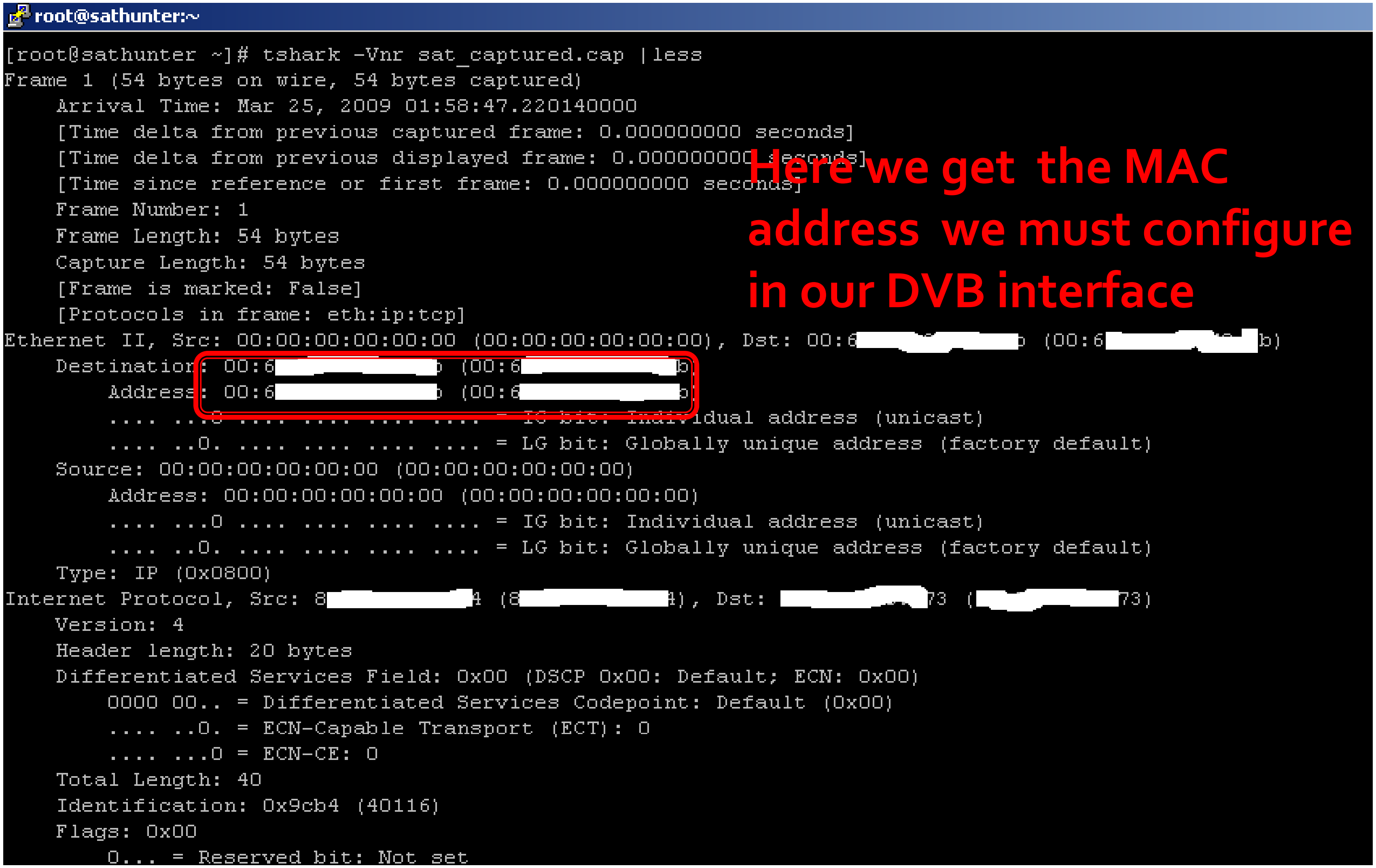
We need our router 's MAC

HTSNACBT Attack

Configure our dvb interface to receive this IP (I suppose that you have configure the PID...)

The IP is the one we have selected and in the ICMP scan, we must get the destination MAC sniffed.

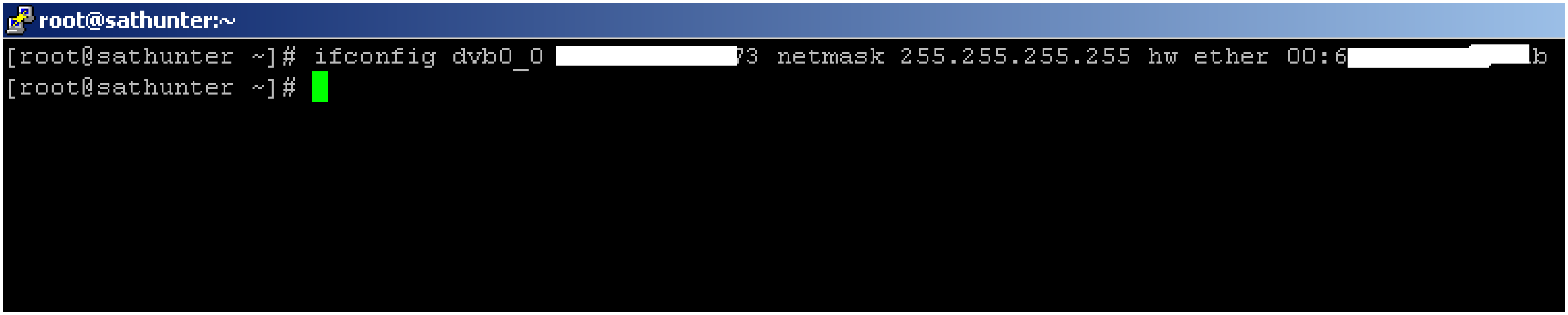
HTSNACBT Attack



```
[root@sathunter ~]# tshark -Vnr sat_captured.cap |less
Frame 1 (54 bytes on wire, 54 bytes captured)
    Arrival Time: Mar 25, 2009 01:58:47.220140000
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 54 bytes
    Capture Length: 54 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:tcp]
Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:6[redacted]b (00:6[redacted]b)
    Destination: 00:6[redacted]b (00:6[redacted]b)
        Address: 00:6[redacted]b (00:6[redacted]b)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Source: 00:00:00:00:00:00 (00:00:00:00:00:00)
        Address: 00:00:00:00:00:00 (00:00:00:00:00:00)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
Internet Protocol, Src: 8[redacted]4 (8[redacted]4), Dst: [redacted]73 ([redacted]73)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 40
    Identification: 0x9cb4 (40116)
    Flags: 0x00
        0... = Reserved bit: Not set
```

Here we get the MAC address we must configure in our DVB interface

HTSNACBT Attack



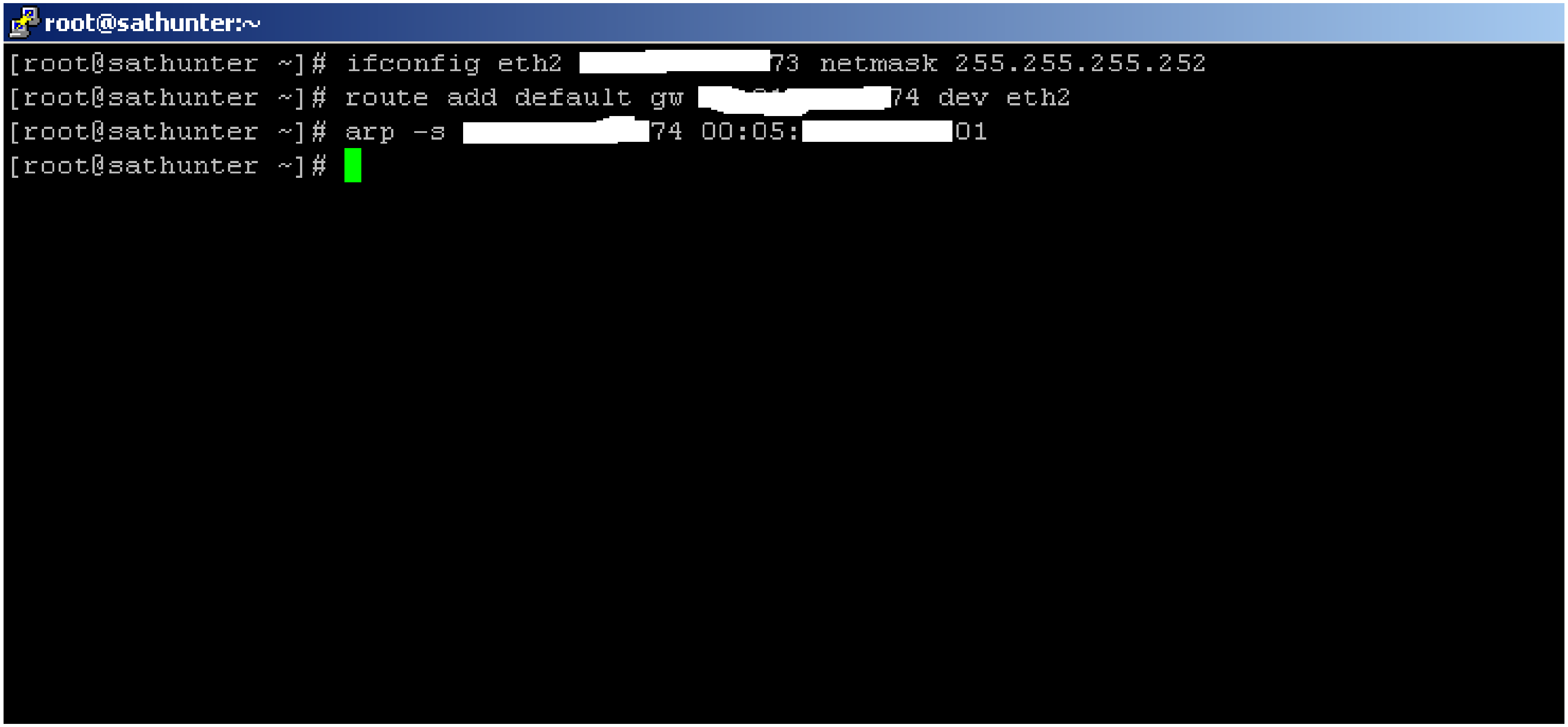
```
[root@sathunter ~]# ifconfig dvb0_0 [redacted]3 netmask 255.255.255.255 hw ether 00:6[redacted]b
[root@sathunter ~]#
```

I use netmask /32 to avoid routing problems

HTSNACBT Attack

Now we can configure our Internet interface with the same IP and configure a default route with a false router setting this one with a static MAC (our real router’s MAC).

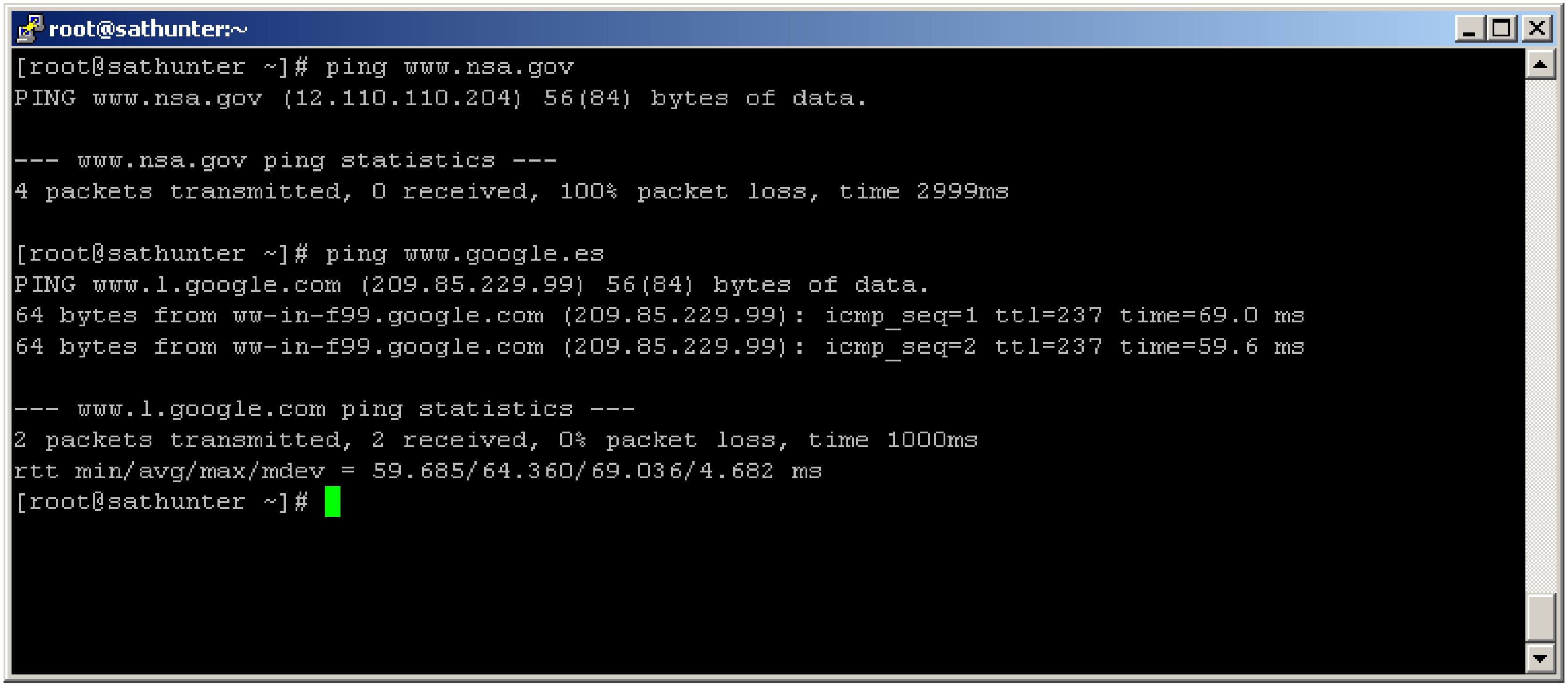
HTSNACBT Attack



```
[root@sathunter ~]# ifconfig eth2 [redacted]73 netmask 255.255.255.252
[root@sathunter ~]# route add default gw [redacted]74 dev eth2
[root@sathunter ~]# arp -s [redacted]74 00:05:[redacted]01
[root@sathunter ~]#
```

HTSNACBT Attack

IT WORKS!



```
[root@sathunter ~]# ping www.nsa.gov
PING www.nsa.gov (12.110.110.204) 56(84) bytes of data.

--- www.nsa.gov ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 2999ms

[root@sathunter ~]# ping www.google.es
PING www.l.google.com (209.85.229.99) 56(84) bytes of data.
64 bytes from ww-in-f99.google.com (209.85.229.99): icmp_seq=1 ttl=237 time=69.0 ms
64 bytes from ww-in-f99.google.com (209.85.229.99): icmp_seq=2 ttl=237 time=59.6 ms

--- www.l.google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 59.685/64.360/69.036/4.682 ms
[root@sathunter ~]# 
```

HTSNACBT Attack

This is all !!!

Some things you must remember:

The DNS server must allow request from any IP or you must use the satellite ISP DNS server.

HTSNACBT Attack

If you have any firewall (iptables) disable it.

All the things you make can be sniffed by others users.

HTSNACBT Attack

Now attacking GRE is very easy, you only need to configure your Linux with IP of one of the routers (the one with the satellite connection) and configure the tunneling.

http://www.google.es/search?rlz=1C1GPEA_en___ES312&sourceid=chrome&ie=UTF-8&q=configuring+GRE+linux

What TODO now?

- I’m studying the different methods to trace illegal users. (I only have a few ideas).

- In the future I would like to study the possibilities of sending data to a satellite via Astromodem (DVB-RCS).

Conclusions

- Satellite communications are insecure.
- It can be sniffed.
- A lot of attacks can be made, I just talked about only few level 4 and level 3 attacks.

Conclusions

- With this technology in our sky, an anonymous connection is possible.
- Many kinds of Denial of Service are possible.

THANK YOU!!!

Questions time