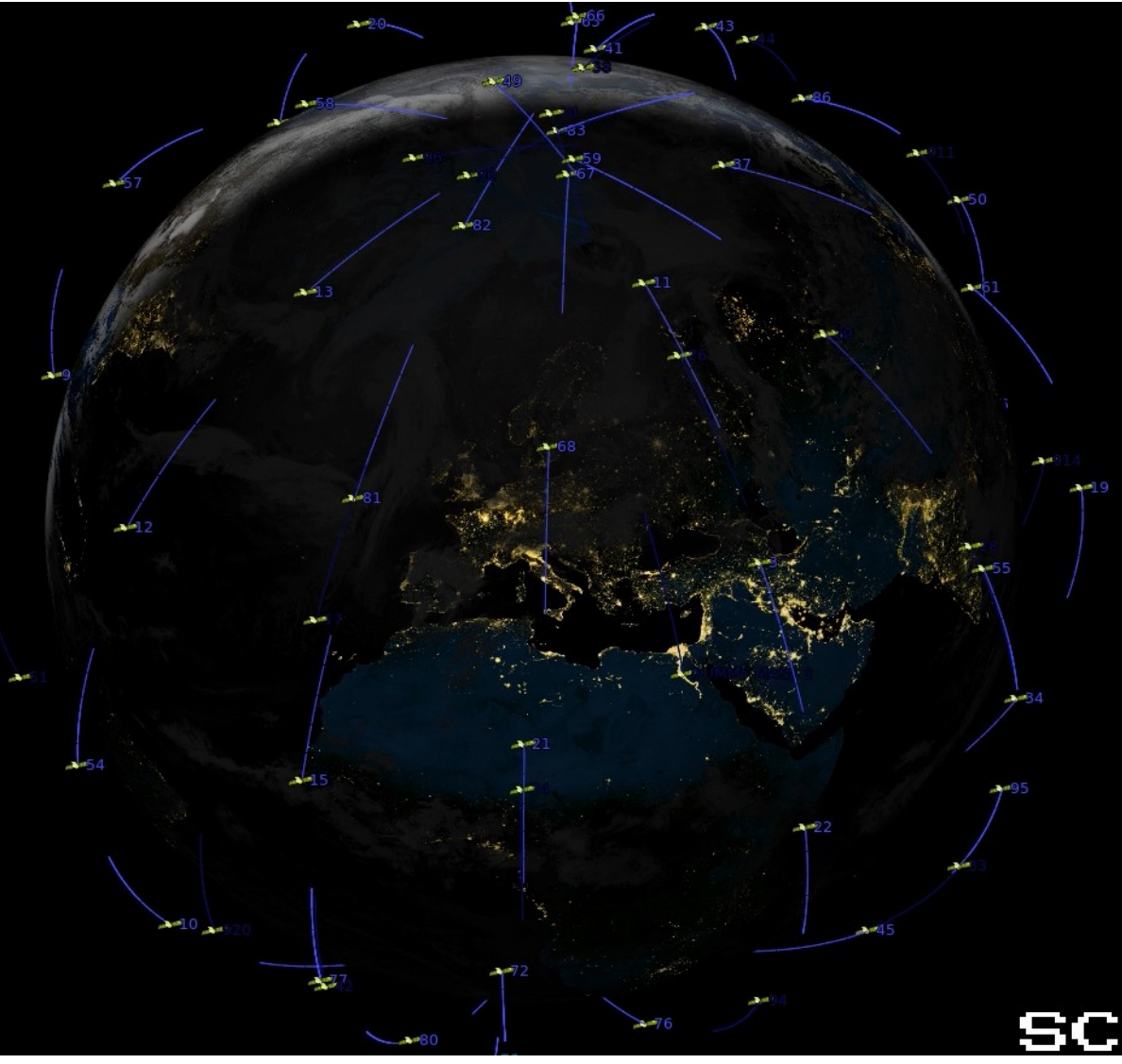
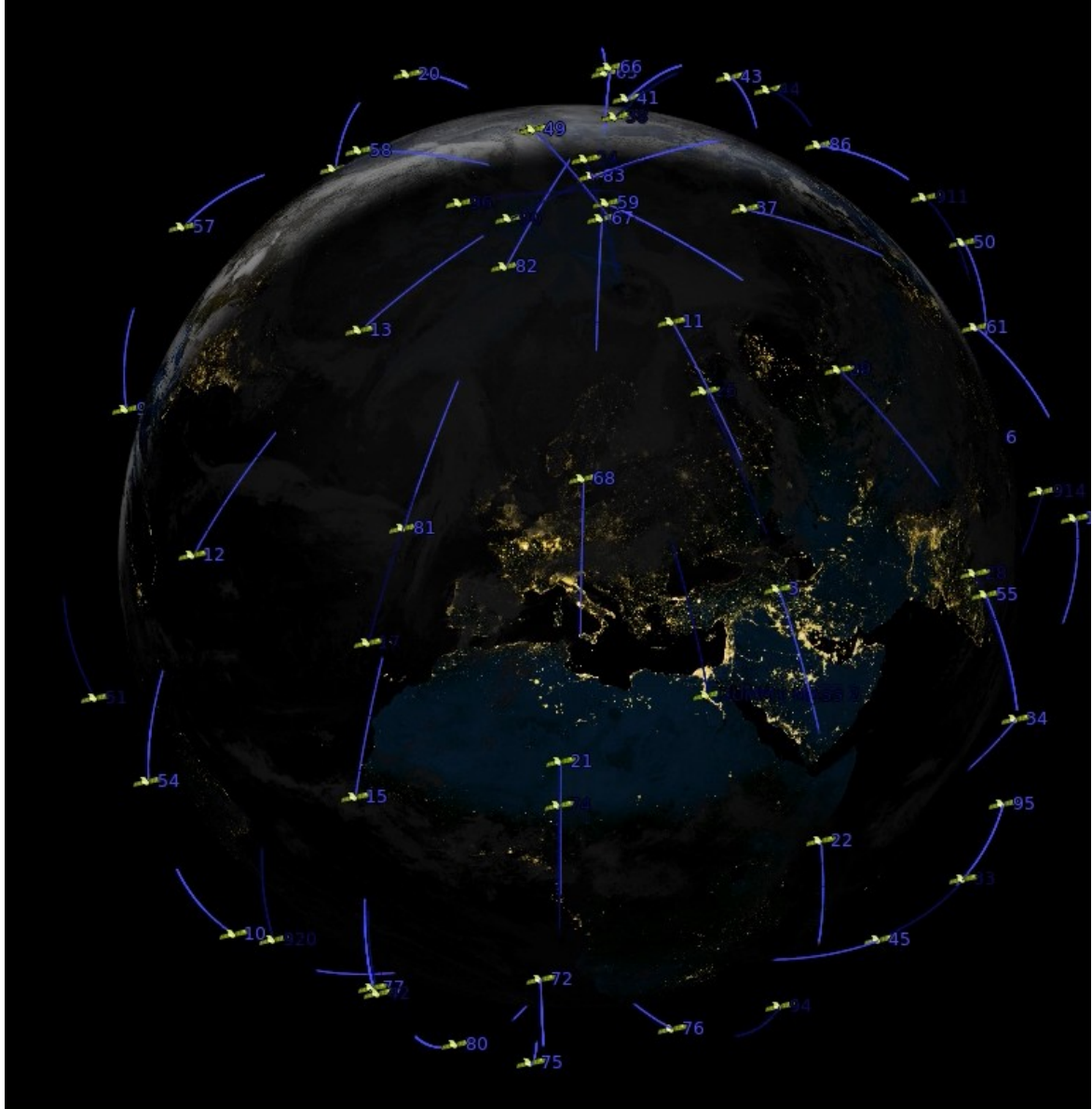
Iridium System Hacking



Sec schneider

What is iridium?

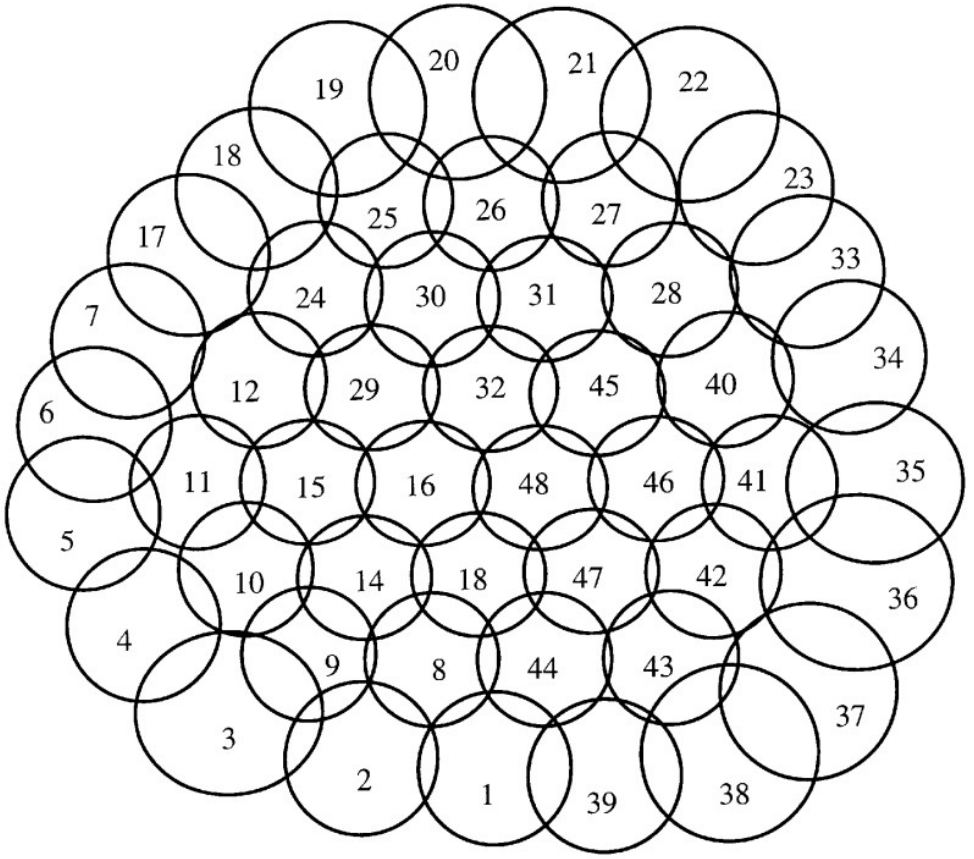
- Built by Motorola in the 90s
- 66 active (logical) satellites
- World-wide coverage
- Services:
  - Messaging
  - Voice
    - very low bit rate
  - Internet/IP/Data



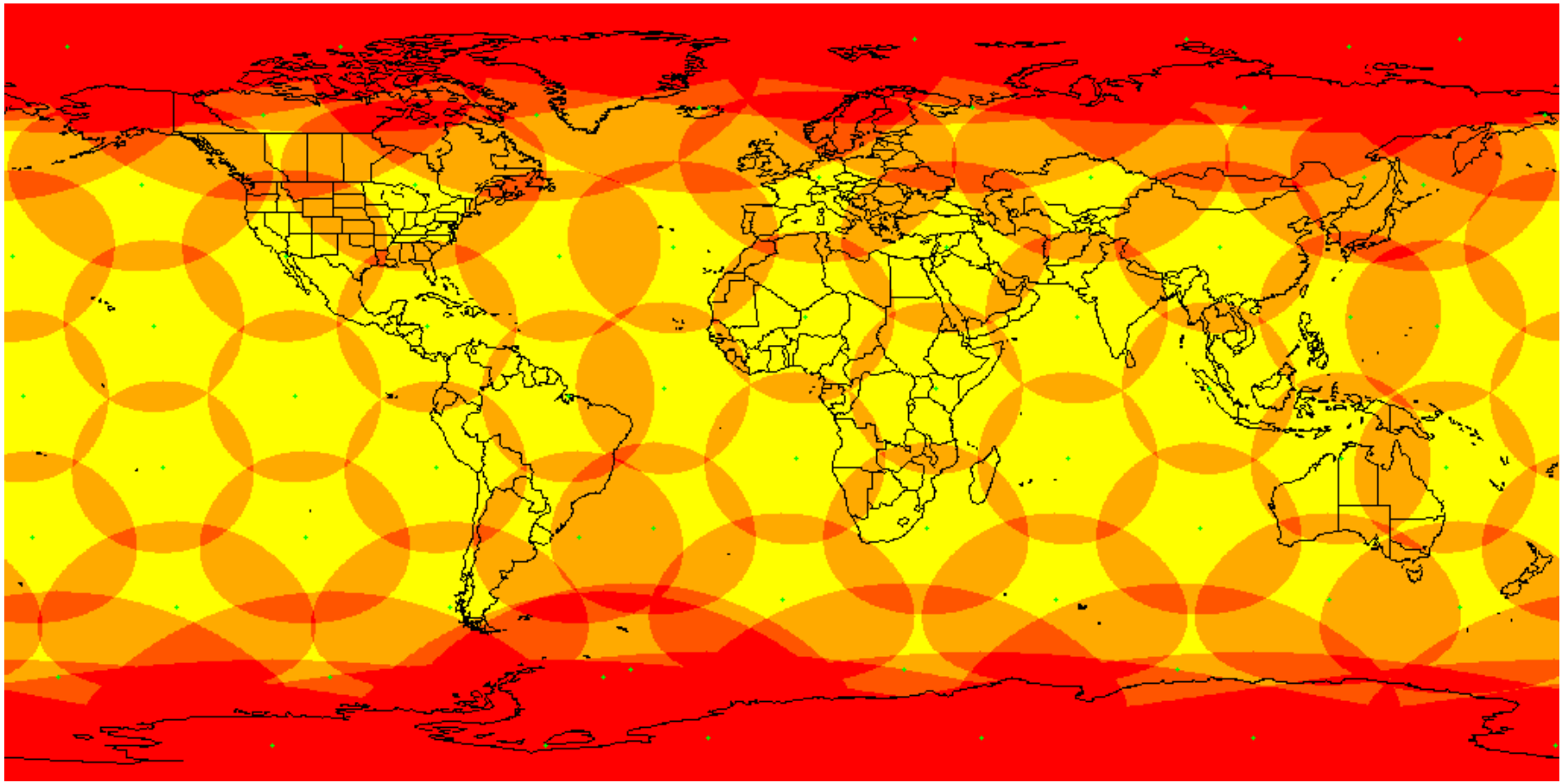
Iridium Coverage

- 4500km ⌀ per satellite
- 48 spot beams
  - ~400km ⌀ spot beam

- With a sensitive setup you can see more than one spot beam



Iridium Coverage



https://commons.wikimedia.org/wiki/File:Iridium_Coverage_Animation.gif

Why look at it?

- There is (almost) no info about it
- World-wide visible
- Low barrier of entry (RTL-SDR)
- Interesting services (Paging, Iridium Burst)
- Future proof (Iridium Next)
  - Scheduled to launch beginning 2016 (backwards compatible)

Applications

- Tracking
- Fleet management
- Mobile Data/Voice
- Emergency services
- Maritime sensors
- Aircraft comms

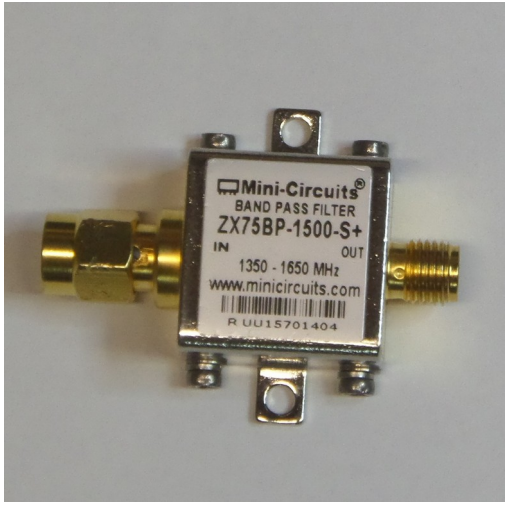
Past work

- In our focus since almost two years
- rad1o: Secret project for ir1dium
- Downlink: demodulation and descrambling
- Pager messages cleartext
- Ring alert and data channel identified

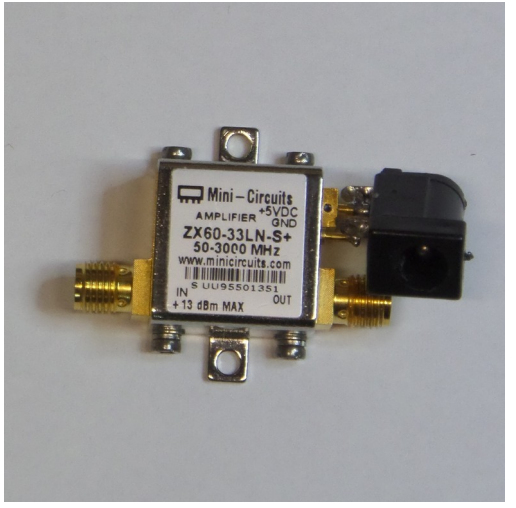
2014-04-20 First idea
2014-05-31 First signal received
2014-10-13 First third party message decoded
2015-05-01 Racal 6103B Testset session
2015-06-08 Received SBD Modem
<rad1o development>
2015-08-13 Talk @ CCCamp
2015-09-17 SBD decoded
2015-10-12 Iridium phone rented
2015-10-14 IP traffic identified
2015-11-14 SBD Modem reversing

Antenna Setup @ 31C3

Passive Iridium Antenna



Bandpass Filter

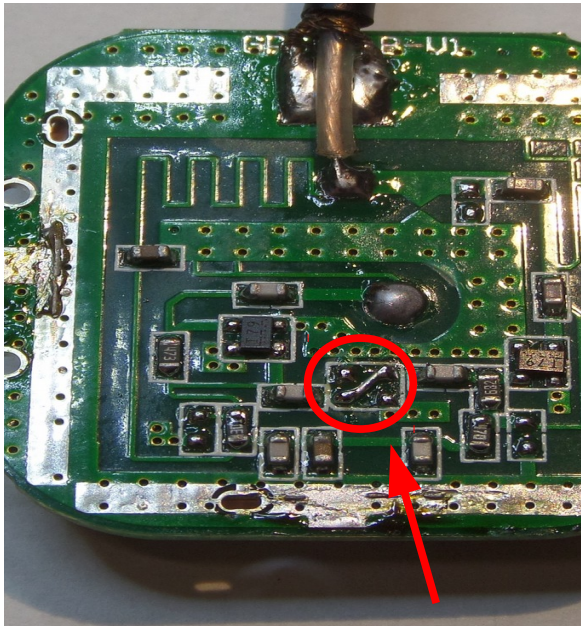


Low Noise Amplifier

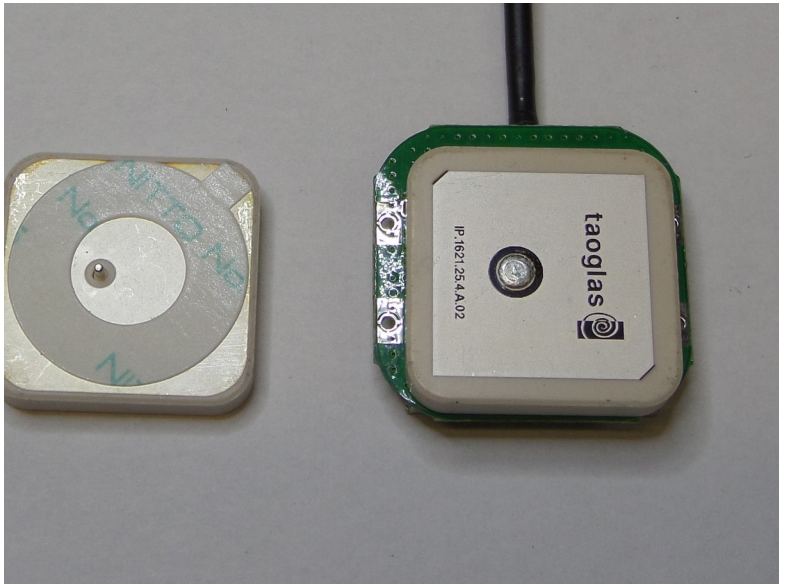
Antenna Setup @ 32C3

- Active GPS antennas serve as a great base
- Modifications:
  - Add Iridium patch antenna
  - Remove GPS filter
  - Optional: Add Iridium filter
- Make sure to get one with screws for easy access

GPS Antenna Modifications



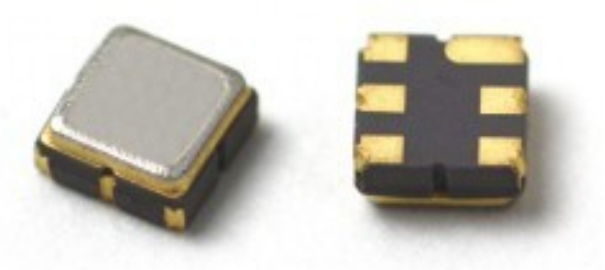
Removed Filter



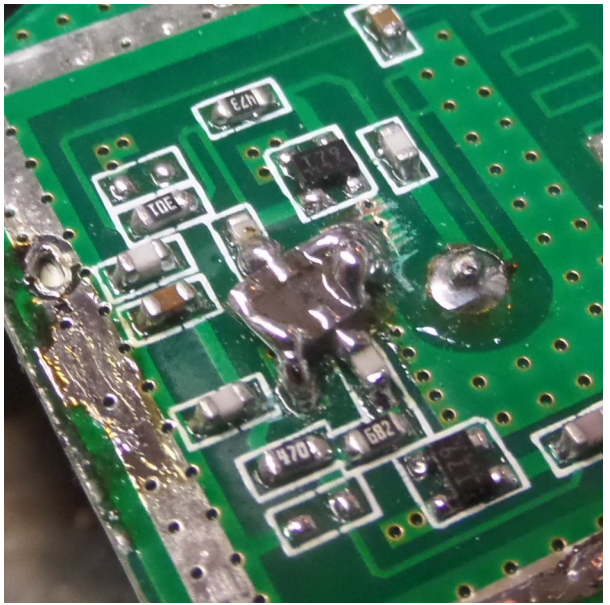
Taoglas IP.1621.25.4.A.02

- See http://wiki.muc.ccc.de/iridium:antennas for more details

GPS Antenna Modifications: Iridium Filter



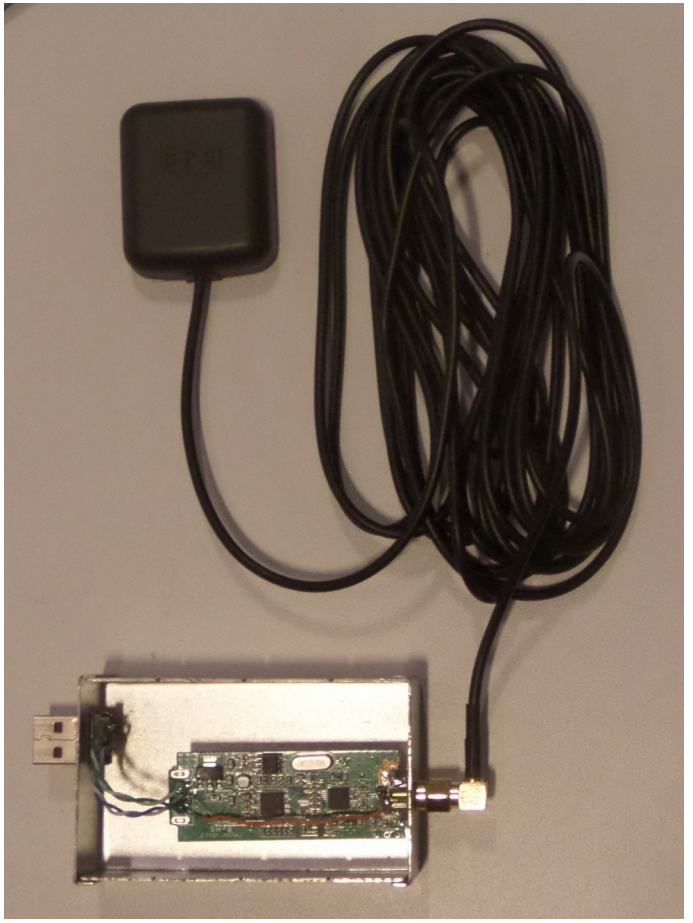
Murata SF2250E-1



- Not strictly needed but highly recommended
- Necessity depends on the RF environment

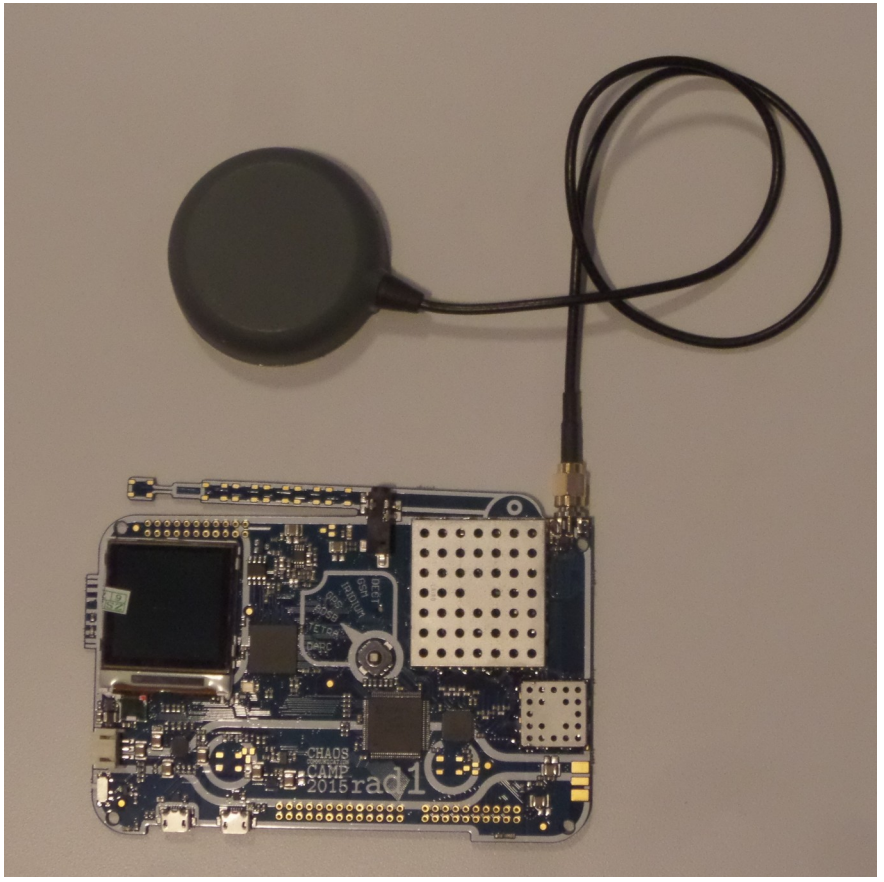
Receiver Setup: RTLSDR + Active Antenna

- Cheapest option
- Can only capture 2-3 MHz
- Needs an E4000 tuner
  - R820(T) do not work reliably at 1600 MHz
- Bias-T modification needed



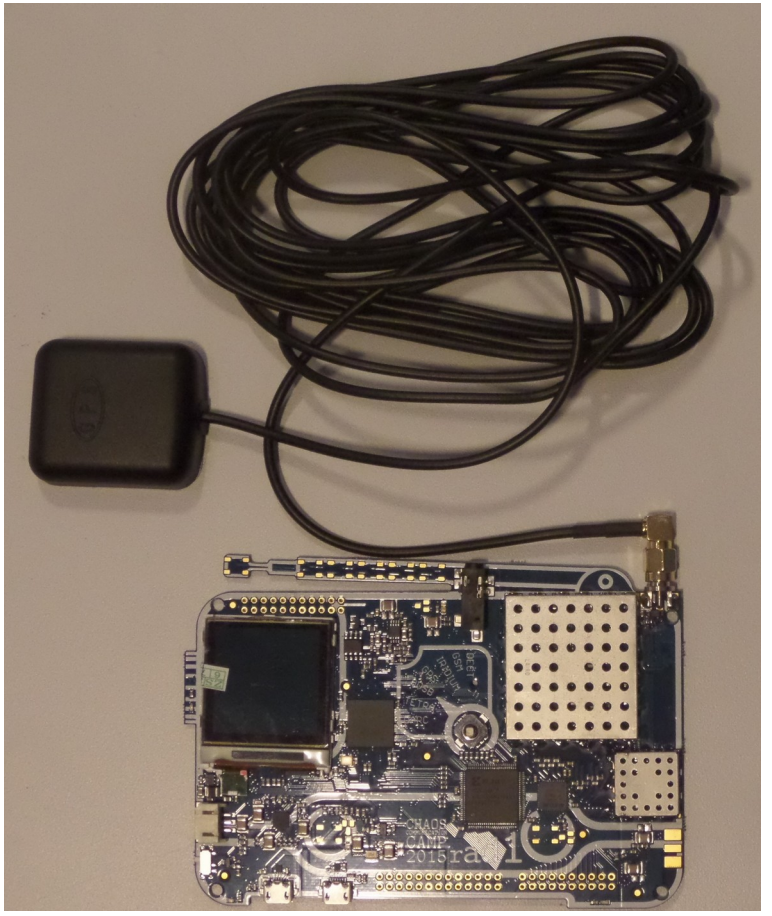
rad1o/USRP/HackRF + Passive Antenna

- Easiest option
- Only works with short cables



rad1o/USRP/HackRF + Active Antenna

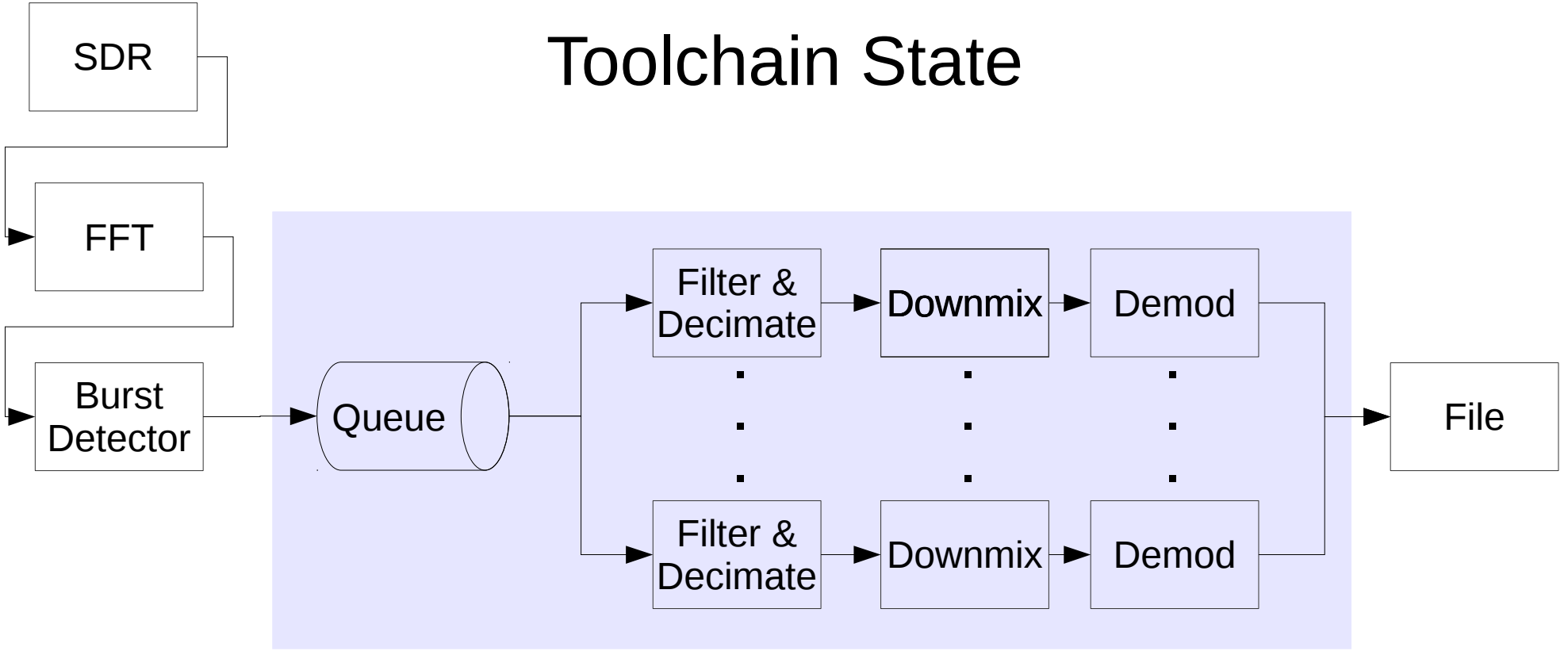
- Best option for reception
- Allows for a longer cable
- SDR can be placed inside a building



Toolchain State

- Improved speed a bit
  - Bursts get filtered and decimated before handling them
  - Uses a faster frequency and phase detection
    - Based on complex correlation with preamble and sync word
- This made processing of the whole Iridium band feasible
- For realtime processing of the whole band, a major improvement is necessary

Toolchain State



- Worker threads can use as many cores as available

Racal 6103 Test Set

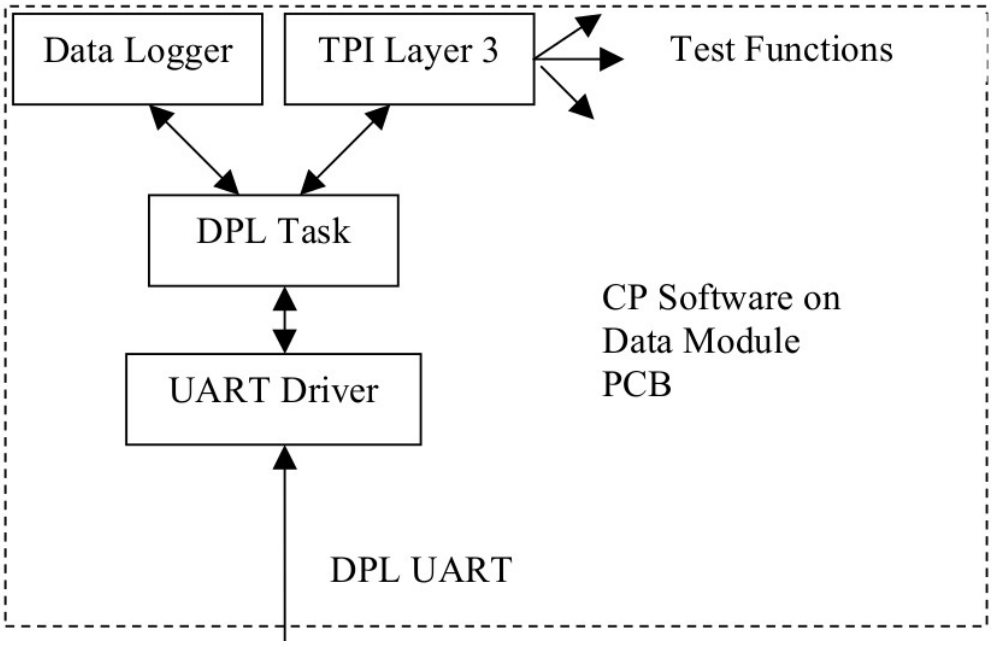
- The Racal test set was a great help
- Thanks to Dieter for reversing the LCW, info about the Broadcast channel and other things

Iridium 9601 SBD Modem

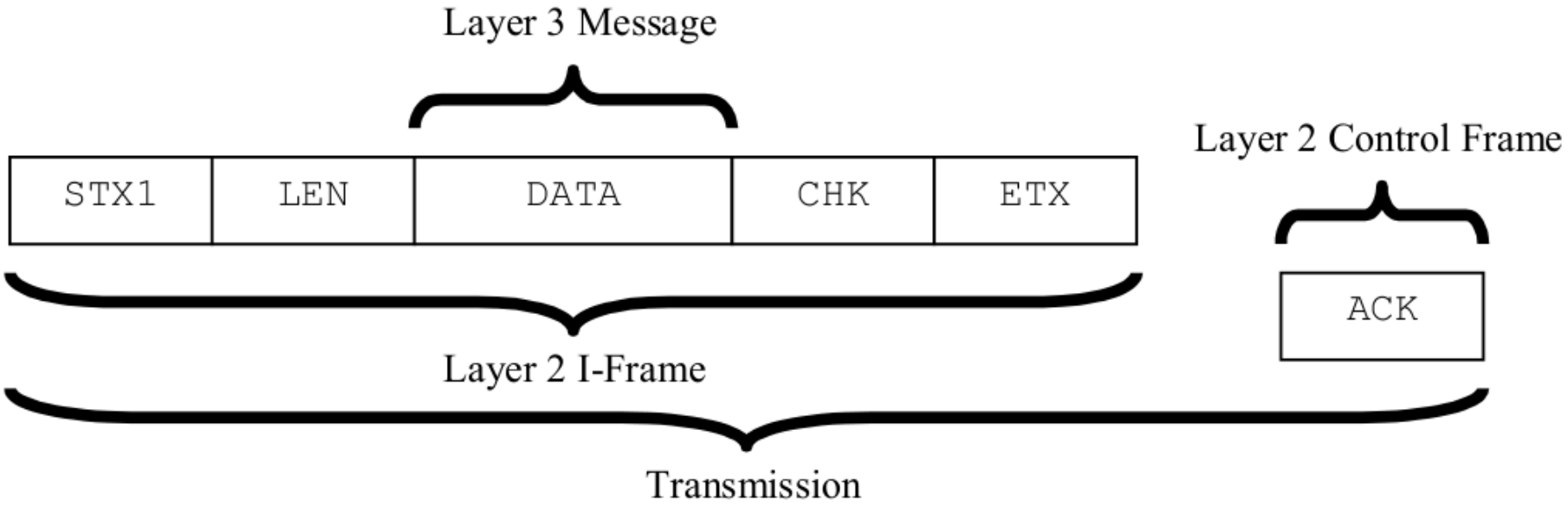
- SteveM got a group order going for a bunch of 9601 modems
  - Cheap batch from ebay
- Simple SBD modem
- Does not use a SIM card
  - Identified by internal IMEI
  - No authentication between network and modem
- To get a contract you need to simply supply the IMEI of a modem

Iridium 9601 SBD Modem

- Test Port Interface (TPI)
  - Sounded rather interesting
- Accessible via the Digital Peripheral Link (DPL)
  - Iridium document C7818-S-013
- No documentation available about TPI



DPL Frame Format



9601 Firmware

- Reversed the firmware to get to the TPI commands

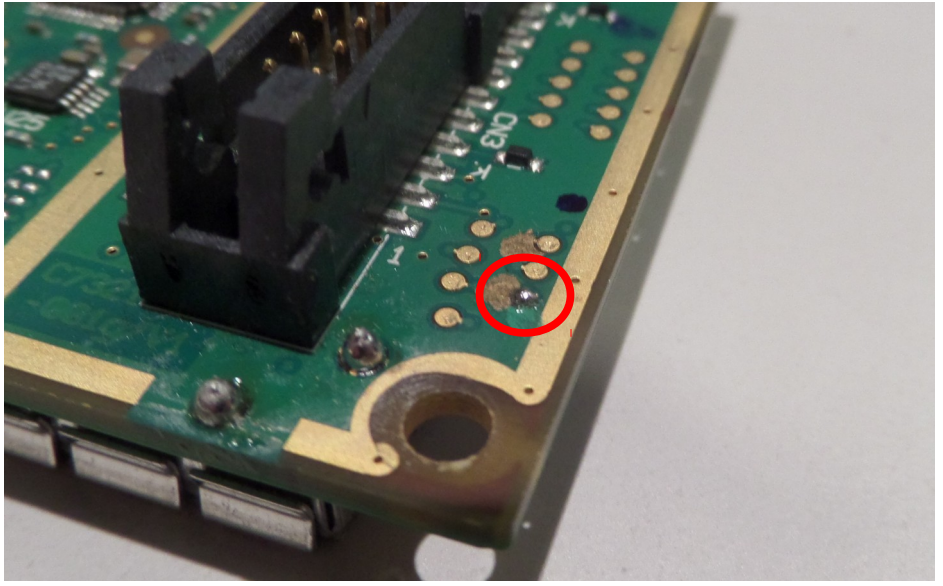
```
ROM:0104DBE4 jpt_1037D5C     struc_3 <tpi_spow,    1, "SPOW",      0,    0>; 0
ROM:0104DBE4                                         ; DATA XREF: tpi_cmd_jumper+30↑o
ROM:0104DBE4                                         ; ROM:off_1037D68↑o ...
ROM:0104DBE4                 struc_3 <tip_srfp,    1, "SRFP",      0,    0>; 1 ; jump table
ROM:0104DBE4                 struc_3 <tpi_e3,    3, "SNDG",      0,    0>; 2
ROM:0104DBE4                 struc_3 <tpi_e3,    3, "SDRB",      0,    0>; 3
ROM:0104DBE4                 struc_3 <tpi_e3,    3, "SDRF",      0,    0>; 4
ROM:0104DBE4                 struc_3 <tpi_e3,    3, "SDRG",      0,    0>; 5
ROM:0104DBE4                 struc_3 <tpi_e3,    3, "SART",      0,    0>; 6
ROM:0104DBE4                 struc_3 <tpi_e3,    3, "SAHR",      0,    0>; 7
ROM:0104DBE4                 struc_3 <tpi_e3,    3, "SBBF",      0,    0>; 8
ROM:0104DBE4                 struc_3 <tpi_e3,    3, "SIFG",      0,    0>; 9
ROM:0104DBE4                 struc_3 <tpi_e3,    3, "PCHR",      0,    0>; 0xA
ROM:0104DBE4                 struc_3 <tpi_e1,    3, "EMMI",      0,    0>; 0xB
ROM:0104DBE4                 struc_3 <tpi_e1,    3, "EMMI",      0,    0>; 0xC
ROM:0104DBE4                 struc_3 <tpi_e1,    3, "EMMI",      0,    0>; 0xD
ROM:0104DBE4                 struc_3 <tpi_e1,    3, "EMMI",      0,    0>; 0xE
ROM:0104DBE4                 struc_3 <tpi_e1,    3, "EMMI",      0,    0>; 0xF
ROM:0104DBE4                 struc_3 <tpi_schn,    1, "SCHN",      0,    0>; 0x10
ROM:0104DBE4                 struc_3 <tpi_sfre,    1, "SFRE",      0,    0>; 0x11
ROM:0104DBE4                 struc_3 <tpi_e1,    3, "SOFF",      0,    0>; 0x12
ROM:0104DBE4                 struc_3 <tpi_e1,    3, "SNGS",      0,    0>; 0x13

0003DBE4 0104DBE4: ROM:jpt_1037D5C
```

DPL/TPI Support

- Partial DPL support:
  - No retransmission or multiple channels yet
- TPI support:
  - ETST: Switch to debug level 1
  - RQEE: Read from EEPROM
    - IMEI, S-Registers, Calibration Data, ...
  - SEEP: Write to EEPROM
    - Change the IMEI of the modem
    - Change debug output flags
- Code on GitHub: 9601/tpi.py

9601 Debug Interface

- Appears on a separate debug UART
- Only available as test points on the PCB
- Off by default
  - Can be enabled by writing to the EEPROM



9601 Debug Output

```
(C) Copyright 2003-5 Cambridge Consultants Ltd
Original code (C) Copyright Motorola 1990
C7321 Talladega Iridium Short Burst Modem
CP version:     TD09004, built: Nov 17 2009 09:55:04
```

9601 Debug Output

RCH_HEADER_CP(Decode=0x0000, SV ID=97, Beam ID=32, X=1009, Y=157, Z=1219, RAI=48, BC slot=1, EPI=0, Subband=14)

RCH_PAYLOAD_CP((TMSI=0x02a22146, MSC/VLR ID=3)(TMSI=0xea619840, MSC/VLR ID=3))

BCCH_HEADER_CP(Decode=0x0000, SV ID=97, Beam ID=32, Slot=1, Acq allowed, Acq classes=0xffff, Acq subband=14, Acq channels=2, TMSI expiration=284264056)

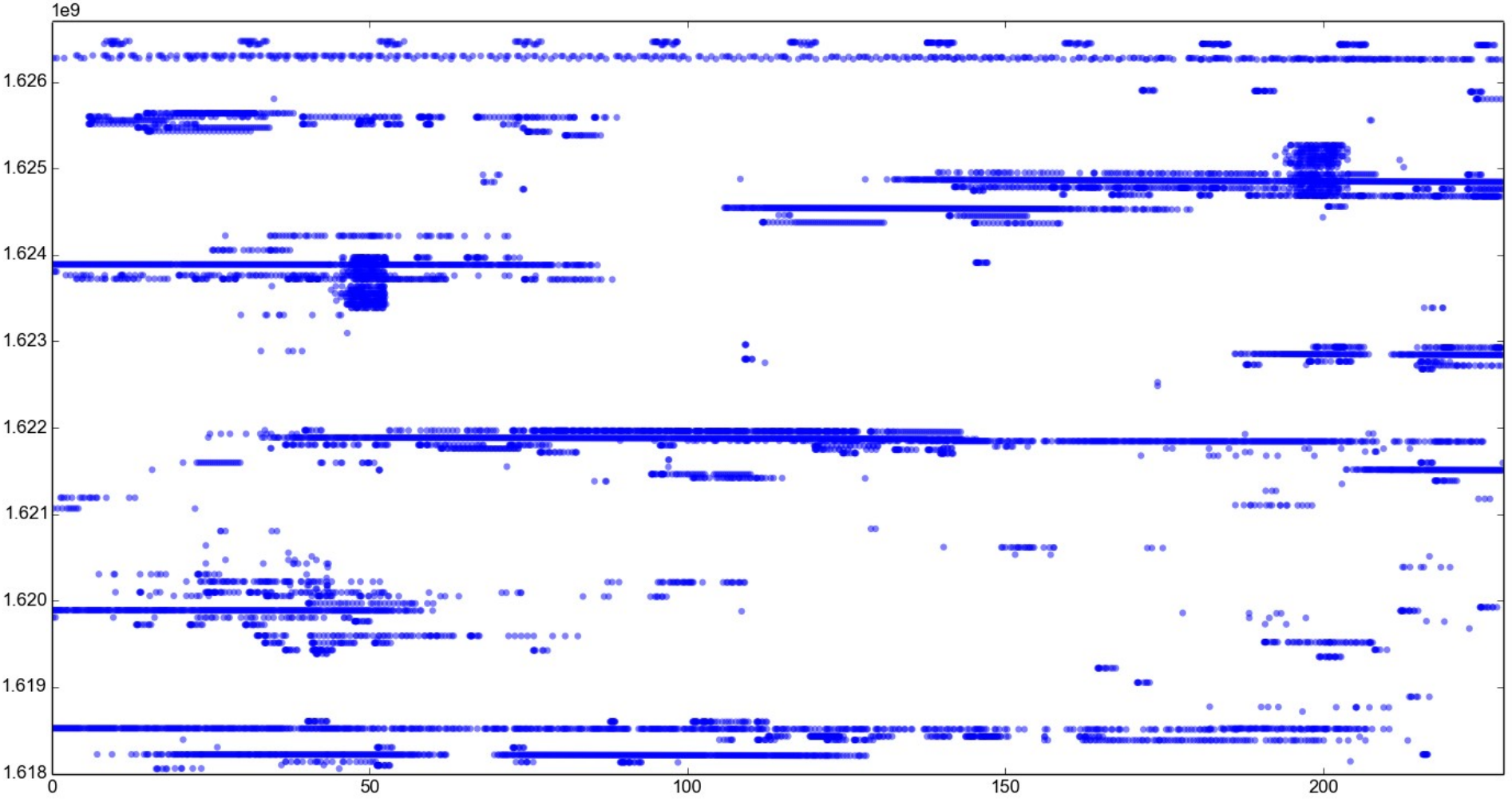
SYNC_HEADER_CP(0x00800400 Type=maint, Code=switch, DTOA=1, DFOA=0)

TCH_HEADER_CP(0x0180fdf8 Type=maint, Code=maint, LQI=0, Power=0, Fine DTOA=63, Fine DFOA=63)

Packets

- Iridium spans 10.5 MHz
  - Between 1.6160 GHz and 1.6265 GHz
  - Current real use in Europe about 8.5 MHz
- We see roughtly 2000 bursts/sec
  - recognized ~ 1200 frames/sec as Iridium
  - Can decode 80% of those without severe errors

Packets


1e9
1.626
1.625
1.624
1.623
1.622
1.621
1.620
1.619
1.618
0
50
100
150
200

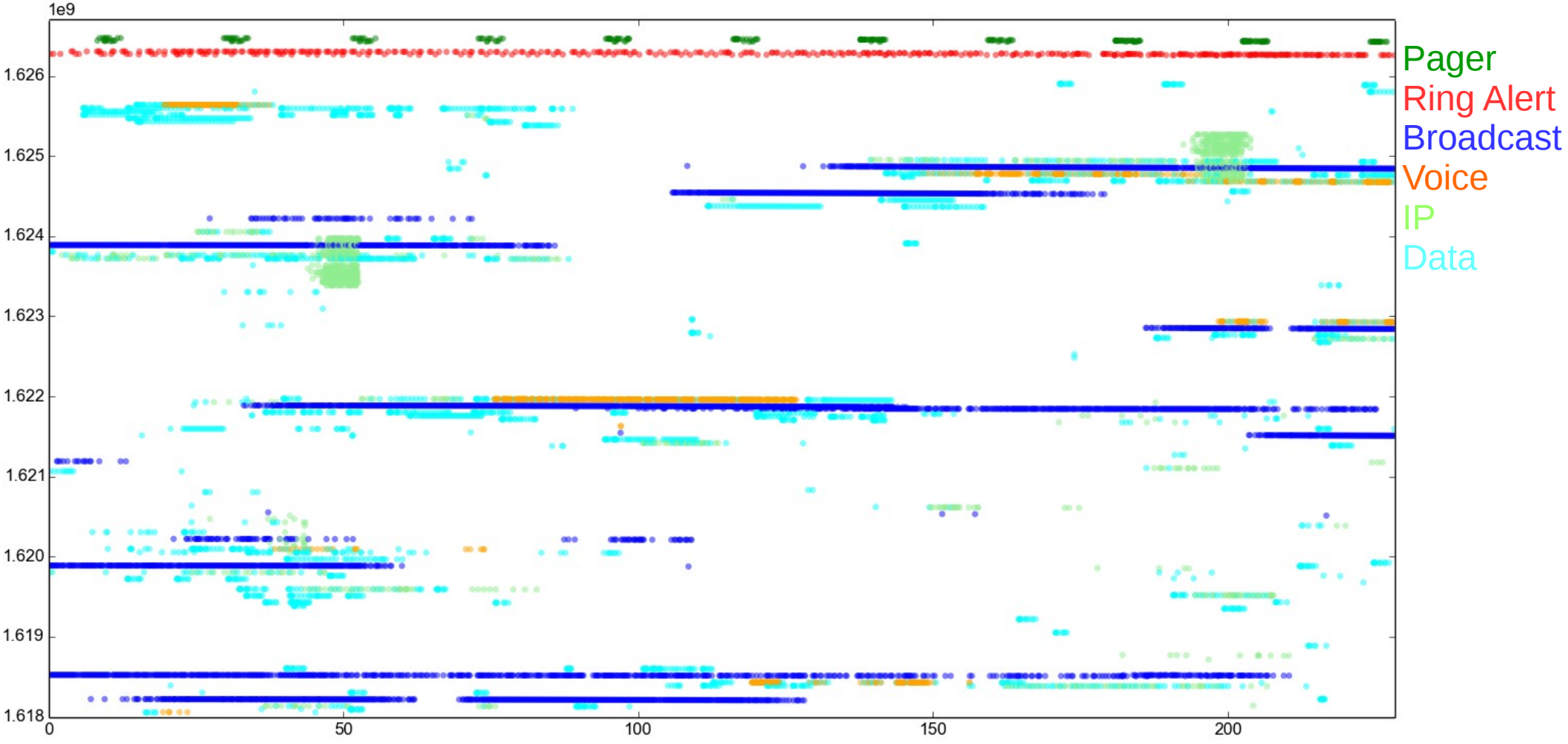
Decoding

- Last year we only looked at pager messages
  - That was 0.5MHz bandwith with way less traffic
- A 4-core Intel I5 (1.2GHz) can decode 2MHz in real time
  - Some ram required to queue bursts / avoid drops
- We think there is room for speed improvements
  - If you're a signal processing guru, maybe you could help?
  - Or maybe some OpenCL support…
- Toolchain supports offline mode
  - Recording @ 12MHz takes 80.5GiB/h or 183Mbit
- Still only looking at downlink
  - Iridium suggests iridium2iridium communications

Frame types

- 4 different frame types
  - Pager messages
  - Ring Alert frames
  - Broadcast frames
  - Data frames

Packets


1e9
1.626
1.625
1.624
1.623
1.622
1.621
1.620
1.619
1.618
0
50
100
150
200
Pager
Ring Alert
Broadcast
Voice
IP
Data

Pager Message Frames

- Frame starts with unique bit pattern (0x9669 in BPSK)

  001100000011000011110011

- Already described in last year's talk

```
2:0:02 ric:0106543 fmt:05 seq:10 1000111010 0/1
schneider@muc.ccc.de
PPPPPPPPPPPPPPPPPPPPPPPPPPPRPPPPPPPPPPPPP
```

Pager Messages

Can I still purchase one-way pagers from Iridium?

- One-way (incoming only) pagers have been out of production for several years. As such, supply is extremely limited. Some of our Service Partners may still have one-way pagers available and will be able to offer Iridium's paging service. Please contact our Service Partners directly for more information.

- Really outdated, but still in use

Ring Alert Frames

- Identified by frequency range
  - 1 626 229 167 < self.frequency < 1 626 312 500
- Format mostly known from reversing the racal test-set firmware
  - Big thanks to Dieter

- Briefly shown at Camp talk

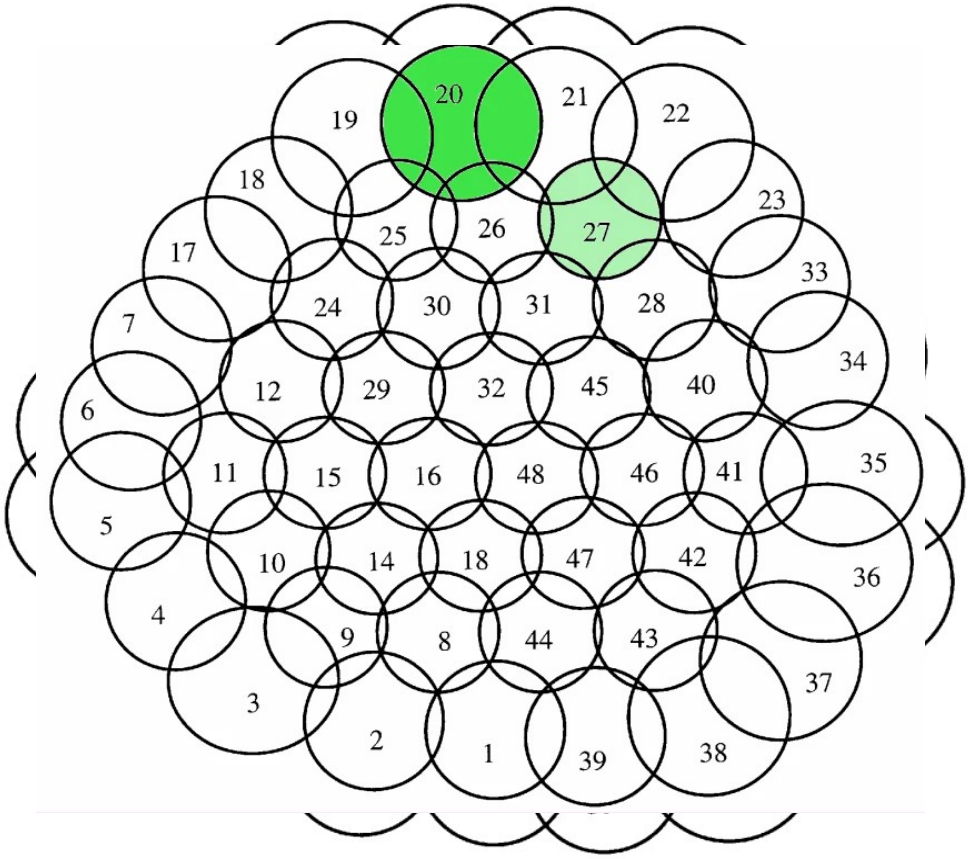
Ring Alert Frames

```
sat:22 beam:25 pos=(+50.9/+012.5) alt=793
RAI:48 ?10 bch:15 PAGE(tmsi:0006a1c6 msc_id:03)
PAGE(tmsi:0cf05ef2 msc_id:03) PAGE(NONE)

sat:22 beam:26 pos=(+39.5/+013.8) alt=010
RAI:48 ?10 bch:14 PAGE(NONE)
```

- Alternating between Position of satellite / center of beam on ground
- Paging TMSI, not IMSI

Ring Alert Beam IDs

- One satellite pass over our receiver



Broadcast Frames

- Identified by valid BCH (1207)
  - Reverse of messaging BCH
- Most info also from racal test-set firmware
- Also briefly shown at Camp talk

Broadcast Frames

```
000000 sat:30 cell:33 0 ts:1 sv_blkn:0
aq_cl:111111111111111 aq_sb:15 aq_ch:2 00 \
000 00000000 ts:0 ul_sb:08 dl_sb:00 000 dtoa:000 dfoa: 00 00
000 00000000 ts:0 ul_sb:00 dl_sb:02 000 dtoa:000 dfoa: 00 00

000000 sat:25 cell:09 0 ts:1 sv_blkn:0
aq_cl:111111111111111 aq_sb:09 aq_ch:2 00
10111010001111111111111110000 max_uplink_pwr:31
```

- Not our focus at the moment

Data Frames

- Identified by valid link control word (LCW)
- Content is always 312 bits long
- LCW consists of three parts
- Most bizarre scrambling seen so far:
  - `[39,40,35,36,31,32,27]`
  - `[28,23,24,19,20,15,16,11,12, 7, 8, 3, 4]`
  - `[42,37,38,33,34,29,30,25,26,21,22,17,18,13,14, 9,10, 5, 6, 1, 2,45,46,43,44,41]`
  - Whoever can explain this to me gets a free beer

Data Frames: LCW

- Each part separatly protected by BCH
  - Separately protected by BCHs
  - `1) BCH(7,4): 29`
  - `2) BCH(13+1,8): 465`
  - `3) BCH(26,5): 41`
- First part of LCW is 3 bit long, we call it „Sub-type“
- Second and third part partially understood from 9601 TPI debug code
  - Contains network related things (maint, acchl, handoff)

Sub-type 7

```
LCW(7,17,96) [55.55.55.55.55.55.55.55
.55.55.55.55.55.55.55.55.55.55.55.55.55
.55.55.55.55.55.55.55.55.55.55.55.55.55
.55.55.55.55.55]
```

- About 43% of all data channel frames
- Probably synchronisation pattern
- Payload is alternating 0 and 1 bits, no other info

```
LCW(7,17,96) SY Sync=OK
```

Sub-type 3

```
LCW(3,44,1775525)
[02.00.0c.09.00.00.00.00.00.00.00.00.00
.00.00.00.00.00.00.00.00.00.00.00.00.00
.00.00.06.91.e2.96.19.bb.3e.1c.8b.bf.82]
```

- About 10% of all data channel fames
- No real idea yet

Sub-type 2

- Roughly 30% of all data frames.
- Descramble as 2 124bit blocks and 1 64bit block.
- BCH checksum with 3545 as polynomial
- Payload has 16bit CRC (CCITT poly: 0x1021)

```
LCW(2,44,619728) 0011 1 ctr=000 0001 0100 0000
[09.01.8f.01.01.07.91.88.61.26.09.00.50.
00.83.24.0e.80.00.88] 004d CRC:OK 0000
```

Sub-type 2 (cont.)

- Payload header contains 3-bit counter
  - used to reassemble longer datagrams

```
0011 1 ctr=000 0001 0100 [09.01.8f.01.01.07.91.88…] CRC:OK
0011 1 ctr=001 0001 0100 [61.26.99.00.00.20.00.51…] CRC:OK
0011 1 ctr=010 0001 0100 [9f.c3.ee.33.48.5f.07.0d…] CRC:OK
0011 1 ctr=011 0001 0100 [66.b3.cb.6d.16.e8.1e.9e…] CRC:OK
0011 1 ctr=100 0001 0100 [b4.0e.bb.dd.2c.d0.3d.5d…] CRC:OK
0011 1 ctr=101 0001 0100 [dd.bd.a6.a7.df.ee.74.59…] CRC:OK
```

Sub-type 2 (cont.)

- 2 byte „Identifier“ at start of datagram
- About 40 different identifiers
- Most are stilll unknown:
  - Those make up about ~ 70%
- Many are „empty“
- Some have no CRC (0000 where the CRC is expected)

Sub-type 2: SMS

- 09.01 contains SMS
- Tested with leased Iridium phone: Iridium 9555

```
0901 8f.01.01.07.91.88.61.26.09.00.50.00.83.24.0e.80.00.88
.61.26.99.00.00.20.00.51.01.51.91.73.12.00.7e.c4.b2.1c.a4.ad
.9f.c3.ee.33.48.5f.07.0d.df.6d.78.9d.5e.96.bb.41.75.37.19.14
.66.b3.cb.6d.16.e8.1e.9e.83.ca.69.77.b9.0d.d2.97.d3.e7.b2.1b
.b4.0e.bb.dd.2c.d0.3d.5d.06.91.d3.e5.79.19.74.2d.b3.e9.20.73
.dd.bd.a6.a7.df.ee.74.59.4e.67.81.e6.6f.36.9b.5e.06.d5.dd.e2
.f2.59.5e.76.eb.e9.a0.ba.9b.0c.b2.bf.d9.ec.39.7d.ef.26.a7.cf
.a0.79.39.ed.76.01.00.00.00.00.00.00.00.00.00.00.00.00.00.00
```

Sub-type 2: SMS

- Structure similar to GSM SMS PDU format

```
0901 SMS: 8f0101 7(91)881662900005 00 83 24
14(80)00881662990000 20 00
15.10.15 19:37:21 {12.00}
```

Sub-type 2: SMS

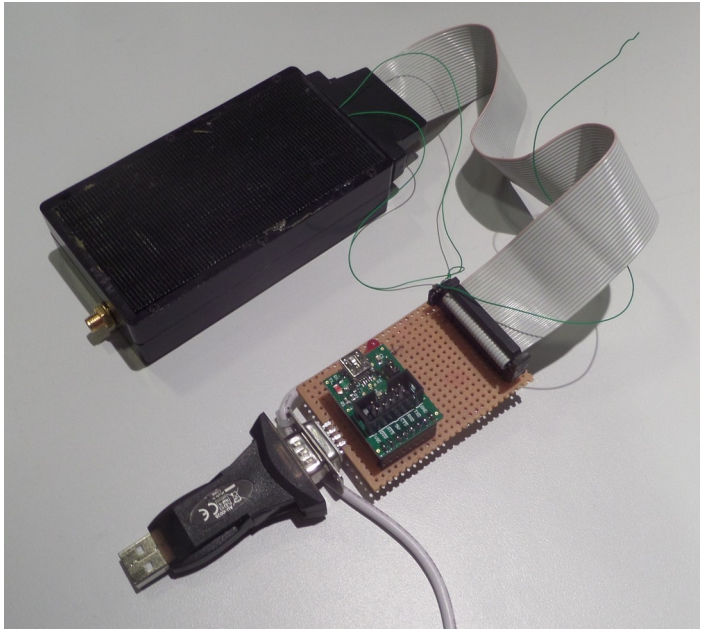
- Structure similar to GSM SMS PDU format

```
0901 SMS: 8f      7(91)881662900005
14(80)00881662990000 20 00
15.10.15 19:37:21
(126) Der Zugang zu Computern und allem, was
einem zeigen kann, wie diese Welt funktioniert,
sollte unbegrenzt und vollständig sein.
00.00.00.00.00.00.00.00.00.00.00.00.00.00
```

- 7bit (GSM 03.38) alphabet.

Sub-type 2: SBD

- 76.08 (and 76.09) contains Short Burst Data messages.
  - 76.09 is for continuation
- SBD can be 1960/1890 (MO/MT) bytes long
- Iridium 9601 SBD modem supports 340/270 (MO/MT) bytes.



SBD Transfer

- E-mail to data@sbd.iridium.com with IMEI in the subject
  - Data to send as attachment
- You can also just define TCP IP:port (both directions)
  - Iridium side has source-ip based firewall
- Many applications also use modem to modem transfer
  - Good for us, as we only see the downlink
- ~$1 per kB

Sub-type 2: SBD

- Some (variable-length) header, then raw message

```
7608 SBD: 26000902002ab9 108701
[ABCDEFGH\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\80\00
\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00
\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00
\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00
\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\01
\02\03\04\05\06] { [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0] }
7609 SBD+: 107402
[\07\08\09\0a\0b\0c\0d\0e\0f\10\11\12\13\00\00\00\00\00\00\00\00\00\00\0
0\00\00\00\00\00\00\01\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\0
0\00\ff\ff\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\80\00Der
Zugang zu Computern und allem, was eine] { [0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0] }
```

Sub-type 2: SBD

- Users include:
  - Moving Map System (ADAC)
  - Thuna Fishing Buoy
  - GPS tracker

    …

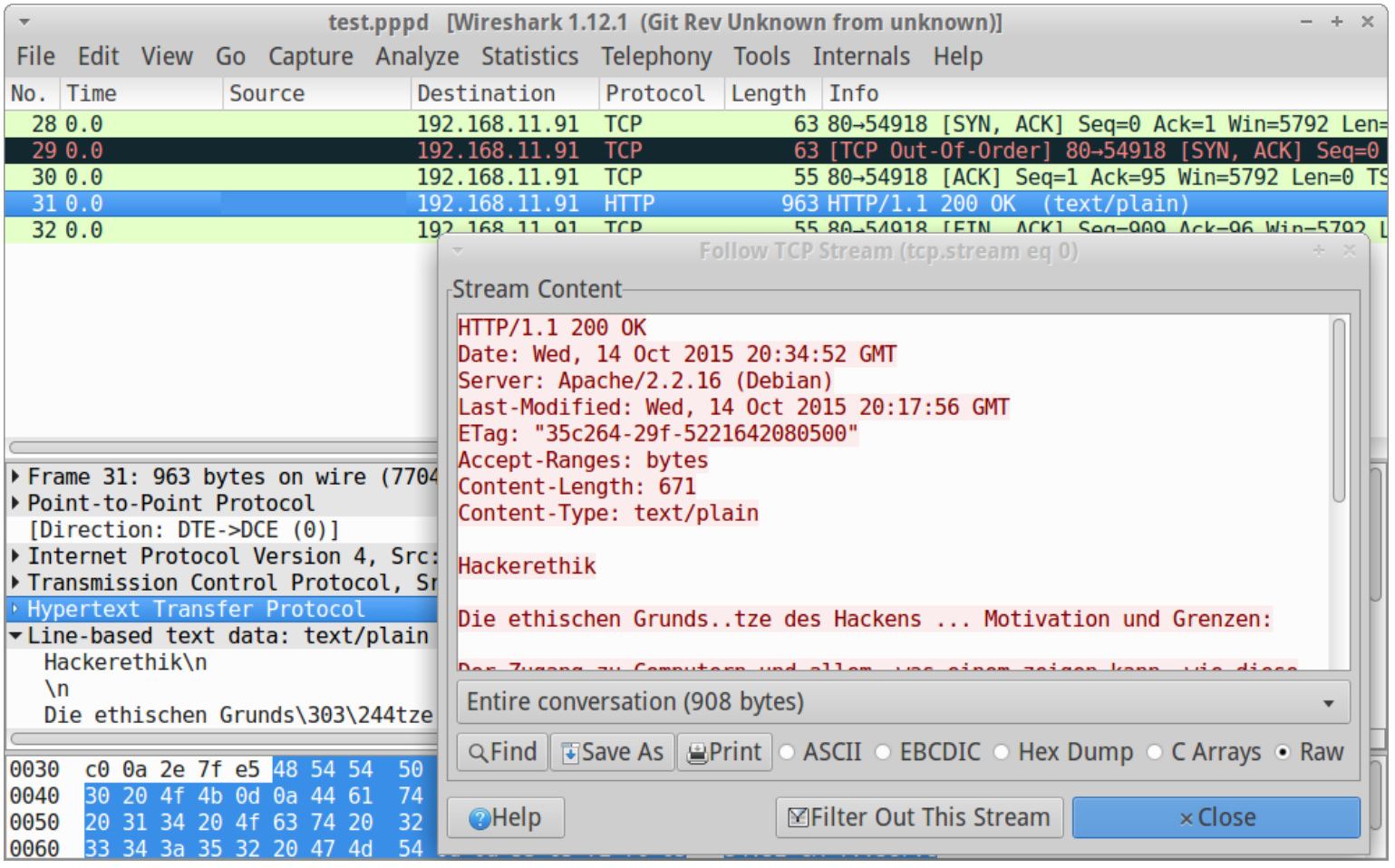
Sub-type 1

- 24bit FCS (CRC with 0xAD85DD / known GSM FCS polynomial)
- Header including 8bit counter for reassembly and length
- Raw data, but bytes are bit-reversed

```
00000100 c1=002 000 c2=249 len=019 […] FCS:OK ~.}#.!}!.} }9}"}&} ...........
00000100 c1=003 000 c2=248 len=031 […] FCS:OK }*} } }#}%.#}%}%}&}$)..}'}"}(}"
00000100 c1=004 000 c2=247 len=003 […] FCS:OK .(~.........................
00000100 c1=005 000 c2=244 len=025 […] FCS:OK ~.}#.!}"}!} }4}"}&} } } }.....
00000100 c1=006 011 c2=242 len=021 […] FCS:OK  }%}&..}%h}'}"}(}"T.~.........
00000100 c1=007 011 c2=241 len=016 […] FCS:OK ~.}#.!}!.} }8}"}.............
```

PPP over serial Link

- It's just IP over PPP
  - Multilink PPP is a possibility
  - Raw „telnet“ also possible
- Wireshark supports pppdump file format
  - http://comments.gmane.org/gmane.linux.ppp/4328
  - Easy to generate
    - assuming you get the packets in the correct order



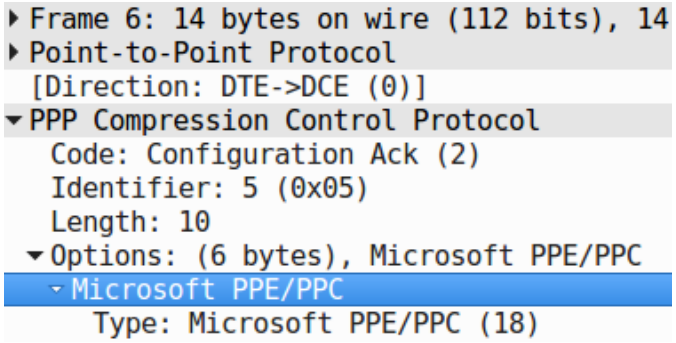
Tested with 9555 phone and Linux

Remember:

Downlink only

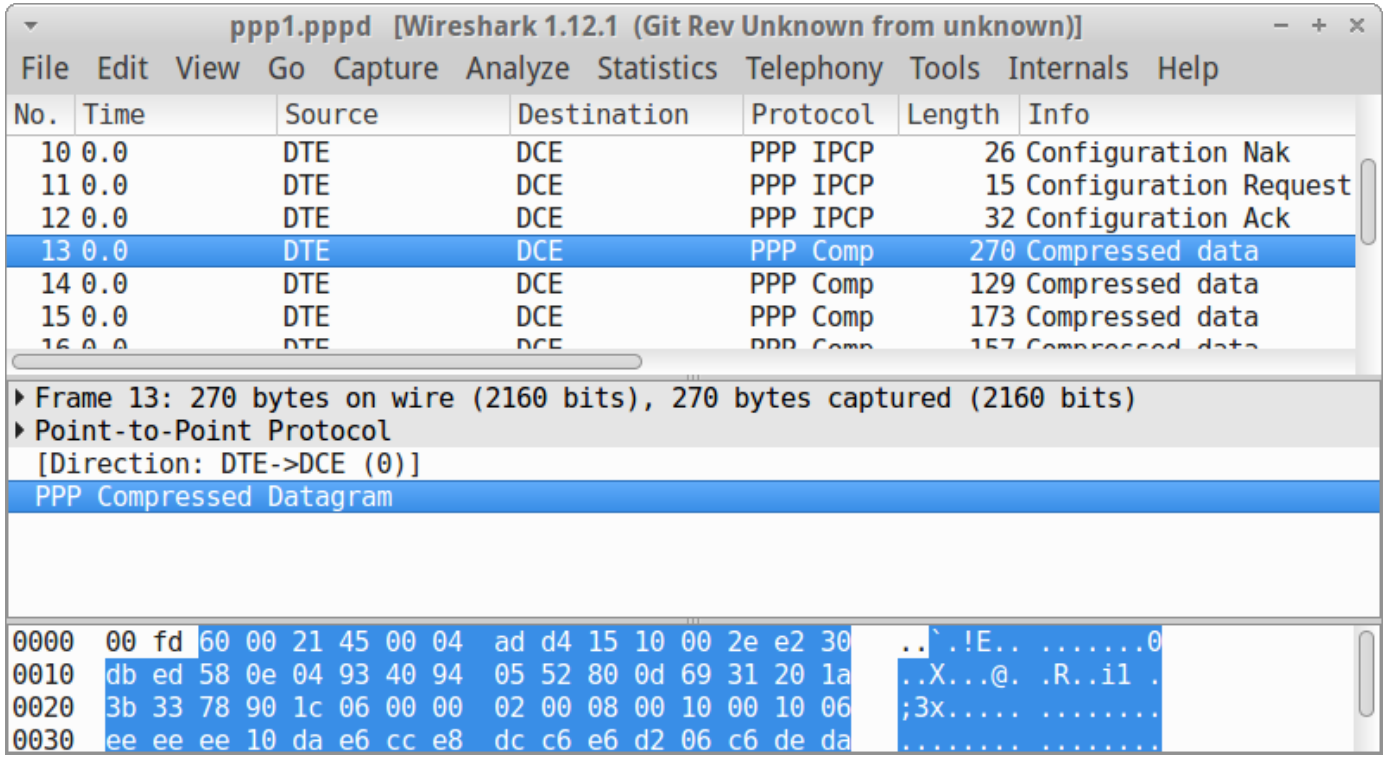
PPP continued

- Nobody uses Linux
- Windows also uses PPP, but



  - Microsoft Point-To-Point Compression (MPPC) Protocol

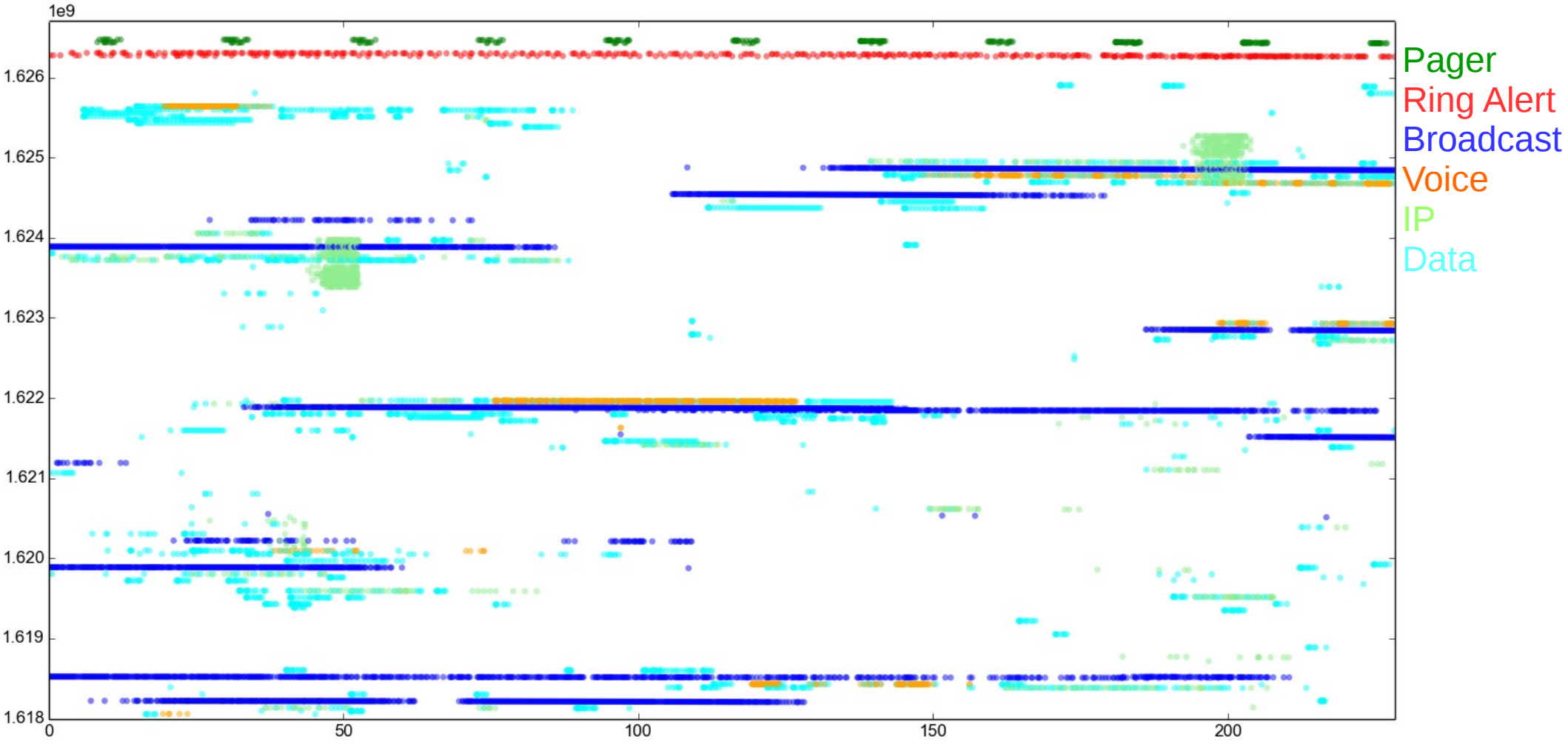
MS PPP Compression



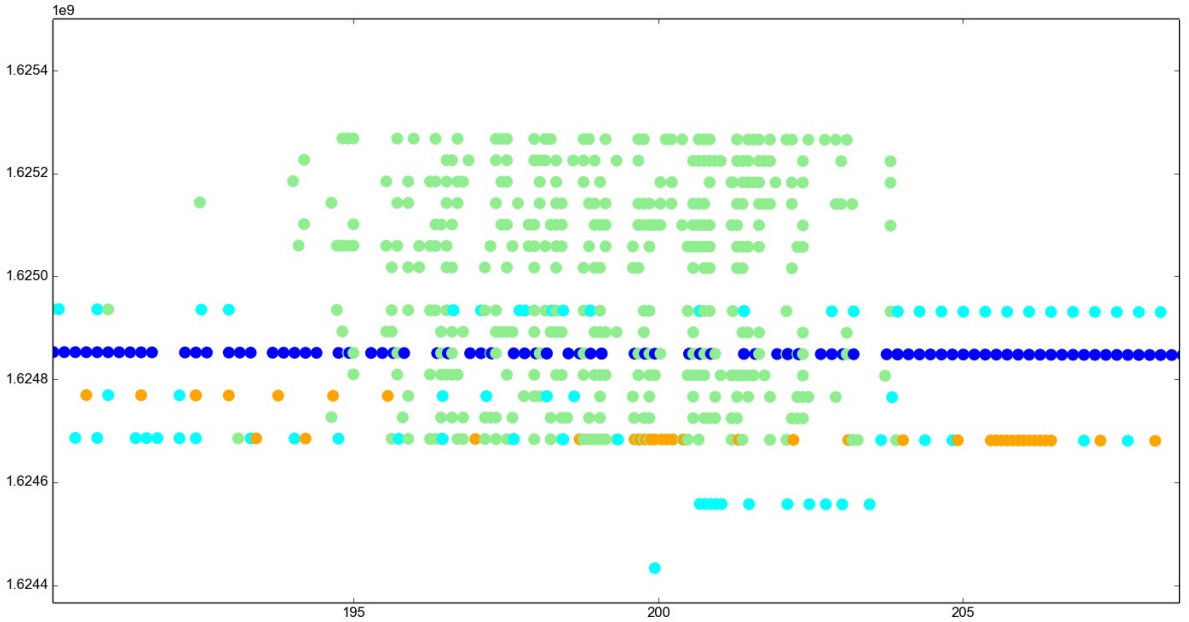
Wireshark can't decode it

MS PPP Compression

- Actually not that difficult
  - RFC 2118
  - Simple back referencing algorithm
    - Problems when packets are missing
- Someone just needs to do it
  - Didn't have time for it (yet)


1e9
1.626
1.625
1.624
1.623
1.622
1.621
1.620
1.619
1.618
0
50
100
150
200
Pager
Ring Alert
Broadcast
Voice
IP
Data

MLPPP



- We've seen up to 14 channels active at the same time
- Likely multilink PPP sessions

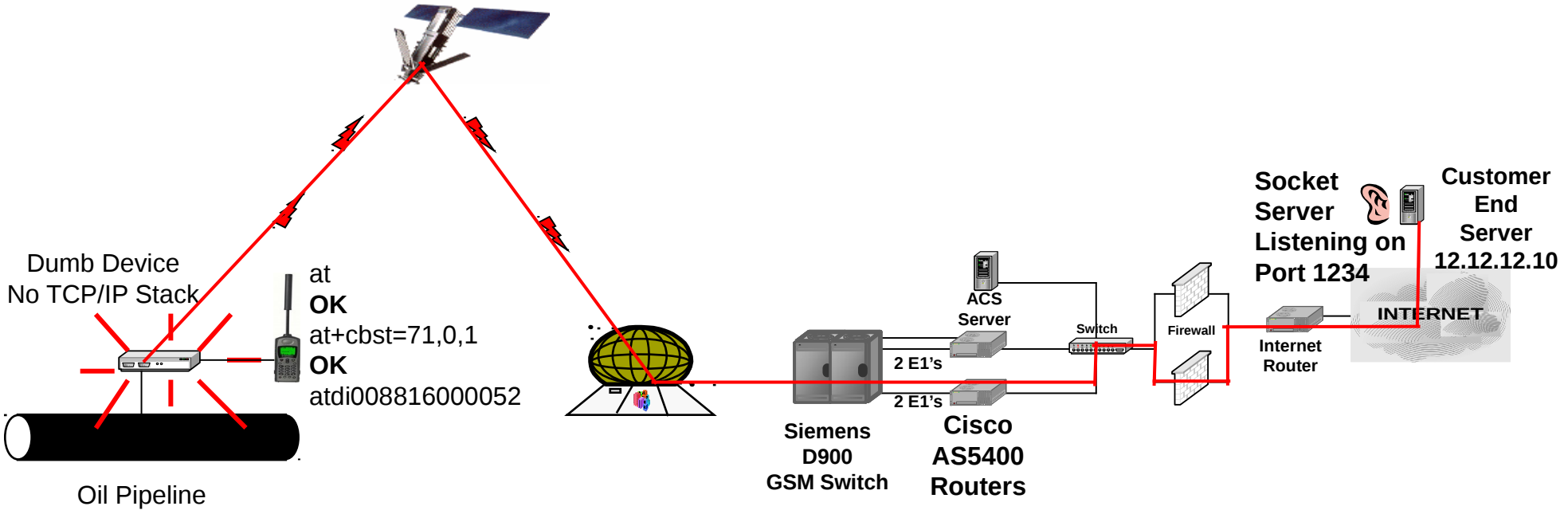
Rudics

- Also non-PPP traffic

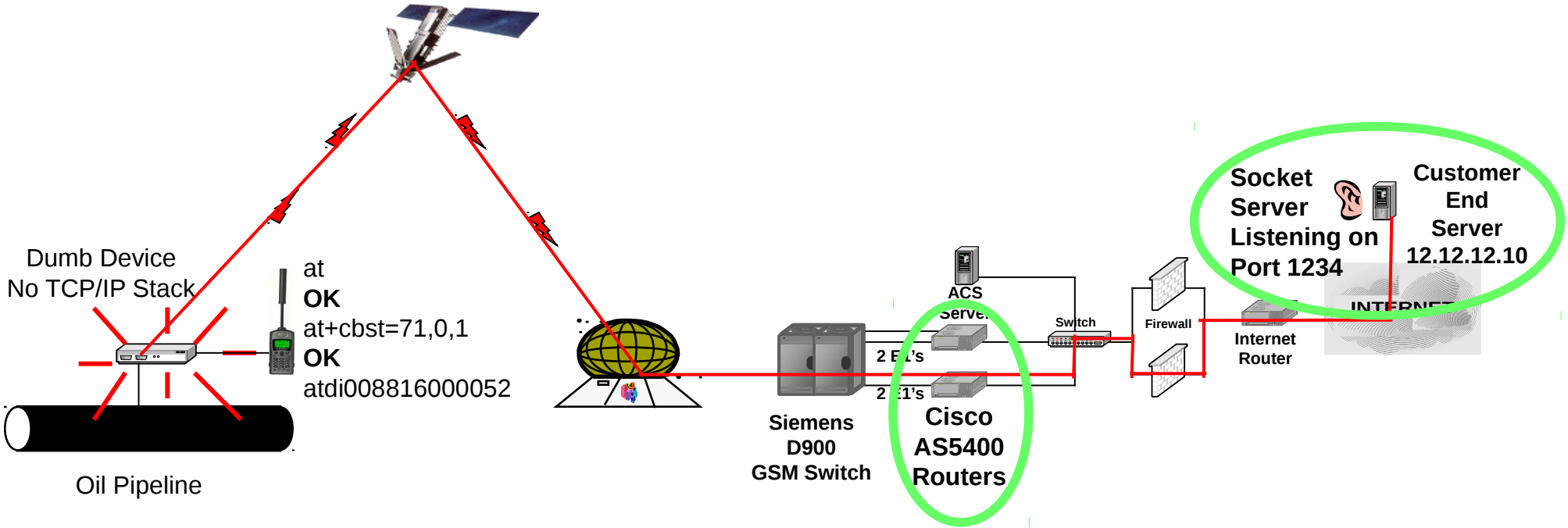
  FCS:OK IP: Trying 193.252.xxx.xxx, 4709 ..
  FCS:OK IP: . Open.....

- Looks like a Cisco …

RUDICS - Basic



RUDICS - Basic



Sub-type 0

- 312 bits of „raw“ Voice data

```
LCW(0,44,1884790)
111100111111111100001111001111001100000000111100000000110000110000000110000000110011001111000011110000000000111100001100000000011000011000000011000000000011110011110011111100110011001111001100110011100111111110000000011000011000000011001111100111110000011000000001111111000000011000001111111000011110011
```

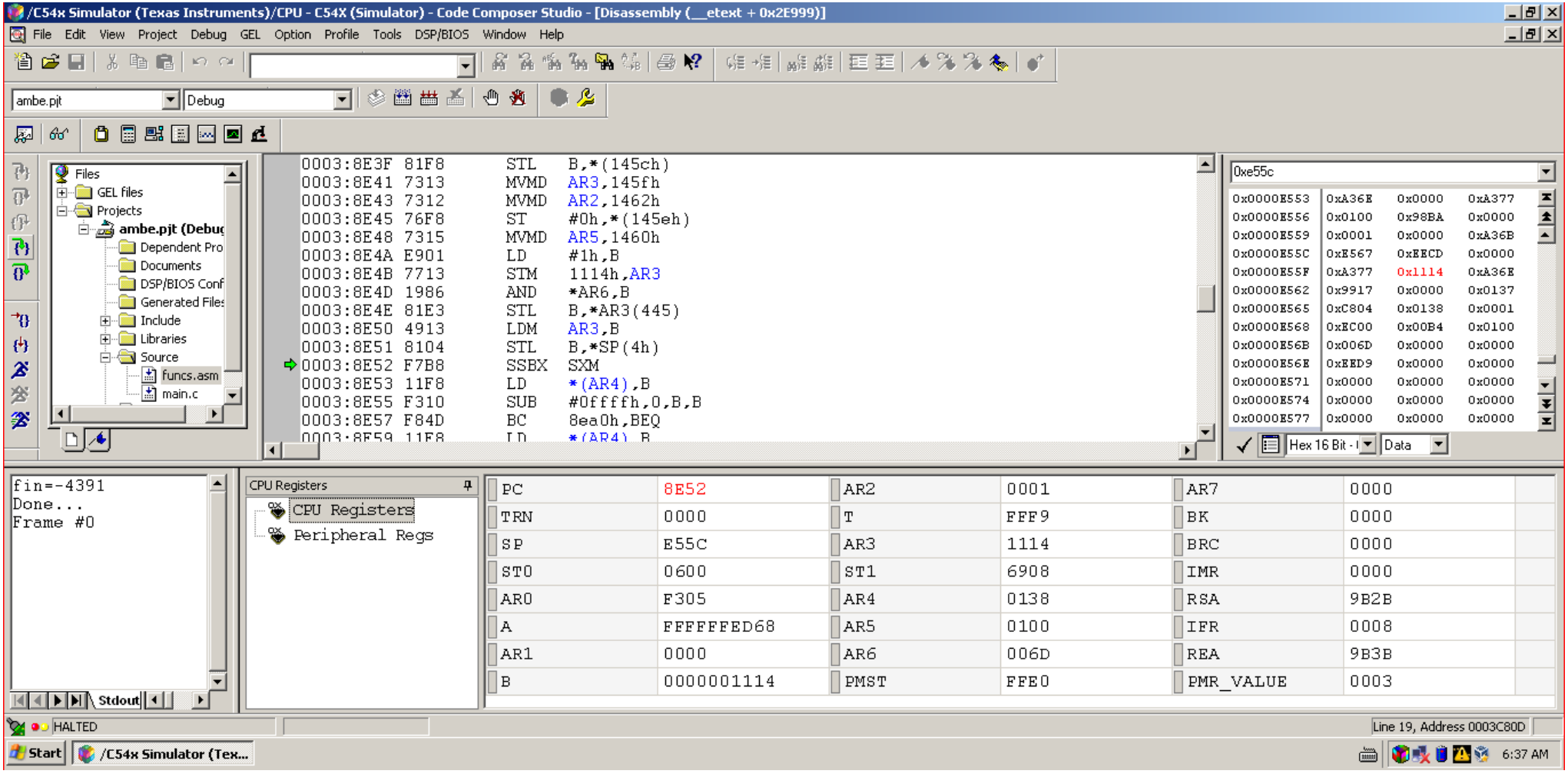
- AMBE voice codec
  - Extremly low bitrate (2400bps)
  - Completely undocumented
- How can we possibly decode this?

Voice Decoding

- Option 1: Other people
  - AMBE is a family of codecs
  - tnt did great work on osmo-gmr and Thuraya
  - See his talk on 31c3:
    - osmo-gmr: What's up with sat-phones ?
      https://events.ccc.de/congress/2014/Fahrplan/events/6267.html
  - Gave him sample files, got iridium version back in record time
    - git://git.osmocom.org/osmo-ir77.git
  - Very fast, good quality

Voice Decoding

- Option 2: Emulation
  - Firmware update of SBD 9601 is available on the internet
    - http://www.idgeurope.com/en/support/firmware-support
  - The voice codec runs on an TI TMS320c5416 DSP chip
    - Very ugly to read assembler code
      - Personal highlight „calld“ / „retd“
  - Supported by an unavailble old version of Code Composer Studio, a Windows emulator/debugging environment.


/C54x Simulator (Texas Instruments)/CPU - C54X (Simulator) - Code Composer Studio - [Disassembly (__etext + 0x2E999)]
File Edit View Project Debug GEL Option Profile Tools DSP/BIOS Window Help
ambe.pjt
Debug
Files
GEL files
Projects
ambe.pjt (Debug
Dependent Pro
Documents
DSP/BIOS Conf
Generated Files
Include
Libraries
Source
funcs.asm
main.c
0003:8E3F 81F8 STL B,*(145ch)
0003:8E41 7313 MVMD AR3,145fh
0003:8E43 7312 MVMD AR2,1462h
0003:8E45 76F8 ST #0h,*(145eh)
0003:8E48 7315 MVMD AR5,1460h
0003:8E4A E901 LD #1h,B
0003:8E4B 7713 STM 1114h,AR3
0003:8E4D 1986 AND *AR6,B
0003:8E4E 81E3 STL B,*AR3(445)
0003:8E50 4913 LDM AR3,B
0003:8E51 8104 STL B,*SP(4h)
0003:8E52 F7B8 SSBX SXM
0003:8E53 11F8 LD *(AR4),B
0003:8E55 F310 SUB #0ffffh,0,B,B
0003:8E57 F84D BC 8ea0h,BEQ
0xe55c
0x0000E553 0xA36E 0x0000 0xA377
0x0000E556 0x0100 0x98BA 0x0000
0x0000E559 0x0001 0x0000 0xA36B
0x0000E55C 0xE567 0xEECD 0x0000
0x0000E55F 0xA377 0x1114 0xA36E
0x0000E562 0x9917 0x0000 0x0137
0x0000E565 0xC804 0x0138 0x0001
0x0000E568 0xEC00 0x00B4 0x0100
0x0000E56B 0x006D 0x0000 0x0000
0x0000E56E 0xEED9 0x0000 0x0000
0x0000E571 0x0000 0x0000 0x0000
0x0000E574 0x0000 0x0000 0x0000
0x0000E577 0x0000 0x0000 0x0000
Hex 16 Bit - I
Data
fin=-4391
Done...
Frame #0
Stdout
CPU Registers
CPU Registers
Peripheral Regs
PC 8E52 AR2 0001 AR7 0000
TRN 0000 T FFF9 BK 0000
SP E55C AR3 1114 BRC 0000
ST0 0600 ST1 6908 IMR 0000
AR0 F305 AR4 0138 RSA 9B2B
A FFFFFFED68 AR5 0100 IFR 0008
AR1 0000 AR6 006D REA 9B3B
B 0000001114 PMST FFE0 PMR_VALUE 0003
HALTED
Line 19, Address 0003C80D
Start
/C54x Simulator (Tex...
6:37 AM

Voice Decoding

- Option 2: Emulation
  - tnt wrote some glue code to get it to run the codec
  - CCS is **slow** (> 1 minute / second)
  - Not really automatable
  - But result is „perfect“ (still crappy bitrate)

Voice Decoding

- Option 3: Translation
  - Reverse engineering requires understanding
  - But maybe we can just „wing it“
    - SPRU131G.pdf (cpu) SPRU172C.pdf describes opcodes
    - Just translate them into crappy C
    - The compiler/optimizer will fix it
  - Enter asm2c.pl

Voice Decoding

```
abs       => sub {
                        return "" if($#_>0);
                        return "set_$_[0](abs($_[0]));if($_[0]==0){SSBX_C;};";
                },
neg       => sub {
                        my $dst=$_[0];
                        $dst=$_[1] if ($#_==1);
                        return "set_$dst(-$_[0]);if($_[0]==0){SSBX_C;}else{RSBX_C;};";
                },
dld       => sub {
                        if ($_[0] =~ /DP(.*)/){
                                return "set_$_[1]( ram[sp $1]<<16|ram[sp $1 +1]);";
                        }elsif($_[0] =~ /\*(.*)([+])$/){
                                return "set_$_[1]( ram[$1]<<16|ram[$1 +1]);$1$2=2;";
                        }elsif($_[0] =~ /\*(.*)/){
                                return "set_$_[1]( ram[$1]<<16|ram[$1 +1]);";
                        }else{
                                return "";
                        };
                 },
subc       => sub {
                        $_[0]=~ s/DP\+(.*)/ram[sp+\1]/;
                        $_[0]=~ s/^\*(.*)\((.*)\)/ram[\1+\2]/;
                        $_[0]=~ s/^\*(.*)/ram[\1]/;
                        return "tmp=$_[1]-(($_[0])<<15);if(tmp>=0){set_$_[1]((tmp<<1)+1);}else{set_$_[1]($_[1]<<1);};";
                 },
```

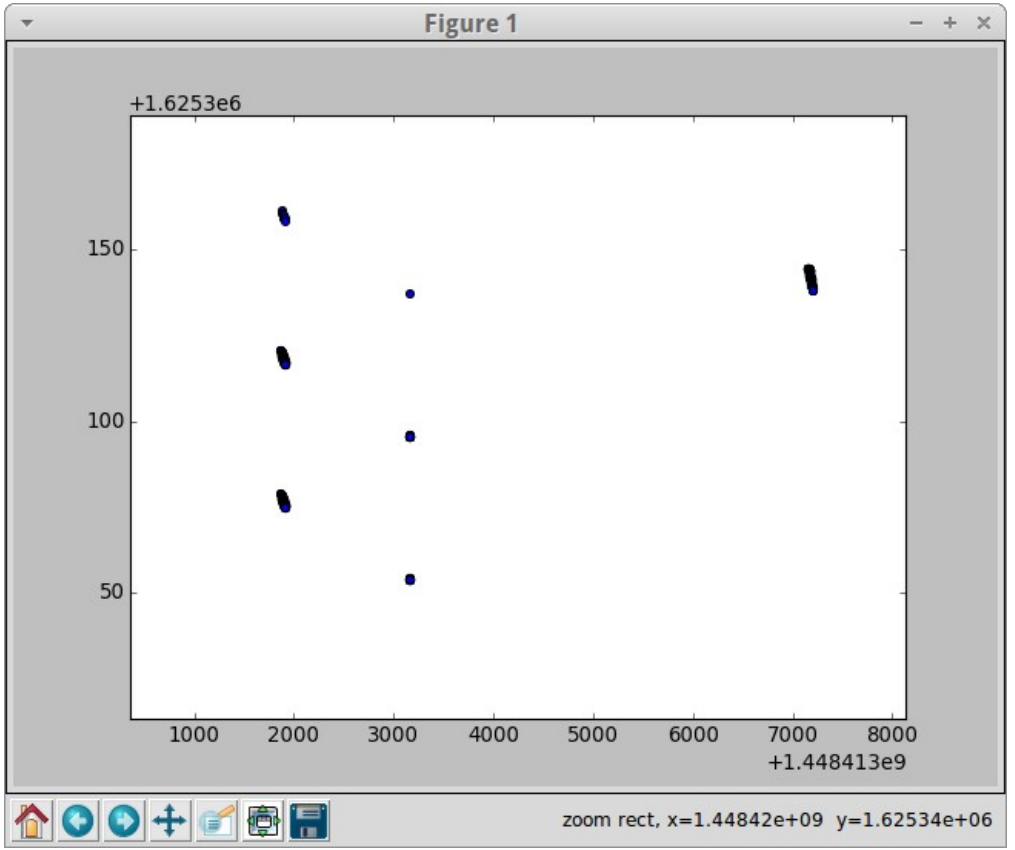
Voice Decoding

- Option 3: Translation
  - Very fast, „perfect“ quality, but not entirely free
  - Shell script to grab necessary binary blob coming soon

Voice Demo

Mystery Data

- Some Data classified as Voice is not decodable
- Typically a bundle of three channels
- AMBE decoder reports <1% valid frames



Range

- If we can see it, everyone can
- Assume that every intelligence agency has all your calls

Iridium Satellite Interception System (ISI)

Main characteristics

SKU	1211
Vendor	**Intercept**
Category	**Intercept**
Standart	**Iridium**
Frequency	**L Band (1616–1626.5MHz)**
System output	**Voice, SMS in all languages, call related data**
Power source	**115/230V AC or 12V DC, 250W**
Active range (m)	**150000**
Battery	**Optional**
SMS(MMS)	**in all languages**
Antenna	**Single, Active, Omni Directional**
Q'ty of channels	**32**
Protocols	**IMEI, TMSI, IMSI**
Management	**API, IP**
Dimensions, HWD	**16.3”x8.9”x12.8"**
Weight	**10 kg**
Shipment	**Worldwide**

ORDERING

Plans

- Look at uplink
  - Far less range
  - Difficult to capture up and downlink at the same time due to signal strength difference
- Pcap/Wireshark
  - Move from ASCII files to format similar to GSMTAP
  - Port some decoding to wireshark modules
- Decoding unknown packets
  - Some voice frames can not be properly decoded
  - Some SBD messages have a binary protocol

Plans

- Signalling, handover & authentication protocol
  - May be necessary to understand to e.g. find IMSI to TMSI mappings
- Further reversing of firmware
  - Telephone and Modem may still hold interesting information
- Performance improvements
- Getting access to more Iridium-related specs and devices

- Code is on github (BSD Licence)
  - https://github.com/muccc/iridium-toolkit
- irc://irc.blafasel.de/#iridium
- If you have access to any iridium-using product/spec
  - We want to play with it
    - Iridium GO
    - OpenPort
    - Any SBD enabled device
    - Iridium Burst
- Thanks to tnt, Dieter and SteveM

<sec@42.org> 26A5 7E7C A201 73FA 8D90 DD96 B86F 0A34 **AB9E 3213**

<schneider@muc.ccc.de> A471 3753 2EC1 E5FF A673 812C 5C85 6CAA **96ED 4C12**

Weltraumtheorie

The leader of the german BND maintains that recording data from satellites does not happen at the point where the receiver is located, but in space, and thus no local (german) law applies to it.

Wie sich herausstellte, ist die Leitung des BND der Meinung, die Datenerhebung finde im Weltraum statt, dort seien ja schließlich die Satelliten. Dort aber würden gar keine Gesetze gelten. Dass die Antennen zur Erfassung der Daten in Bad Aibling in Bayern stehen, sei unerheblich.

- http://www.zeit.de/politik/deutschland/2014-11/bnd-bundesnachrichtendienst-gesetz-grundrecht

Weltraumtheorie

The leader of the german BND maintains that recording data from satellites does not happen at the point where the receiver is located, but in space, and thus no local (german) law applies to it.

Wie sich herausstellte, ist die Leitung des BND der Meinung, die Datenerhebung finde im Weltraum statt, dort seien ja schließlich die Satelliten. Dort aber würden gar keine Gesetze gelten. Dass die Antennen zur Erfassung der Daten in Bad Aibling in Bayern stehen, sei unerheblich. Fand die Datenschutzbeauftragte zwar nicht, aber sie sei "überstimmt" worden, sagte sie.

- http://www.zeit.de/politik/deutschland/2014-11/bnd-bundesnachrichtendienst-gesetz-grundrecht