Worldwide attacks on SS7 network

P1 Security – Hackito Ergo Sum 26th April 2014

Pierre-Olivier Vauboin (po@p1sec.com)

Alexandre De Oliveira (alex@p1sec.com)

Agenda

Overall telecom architecture

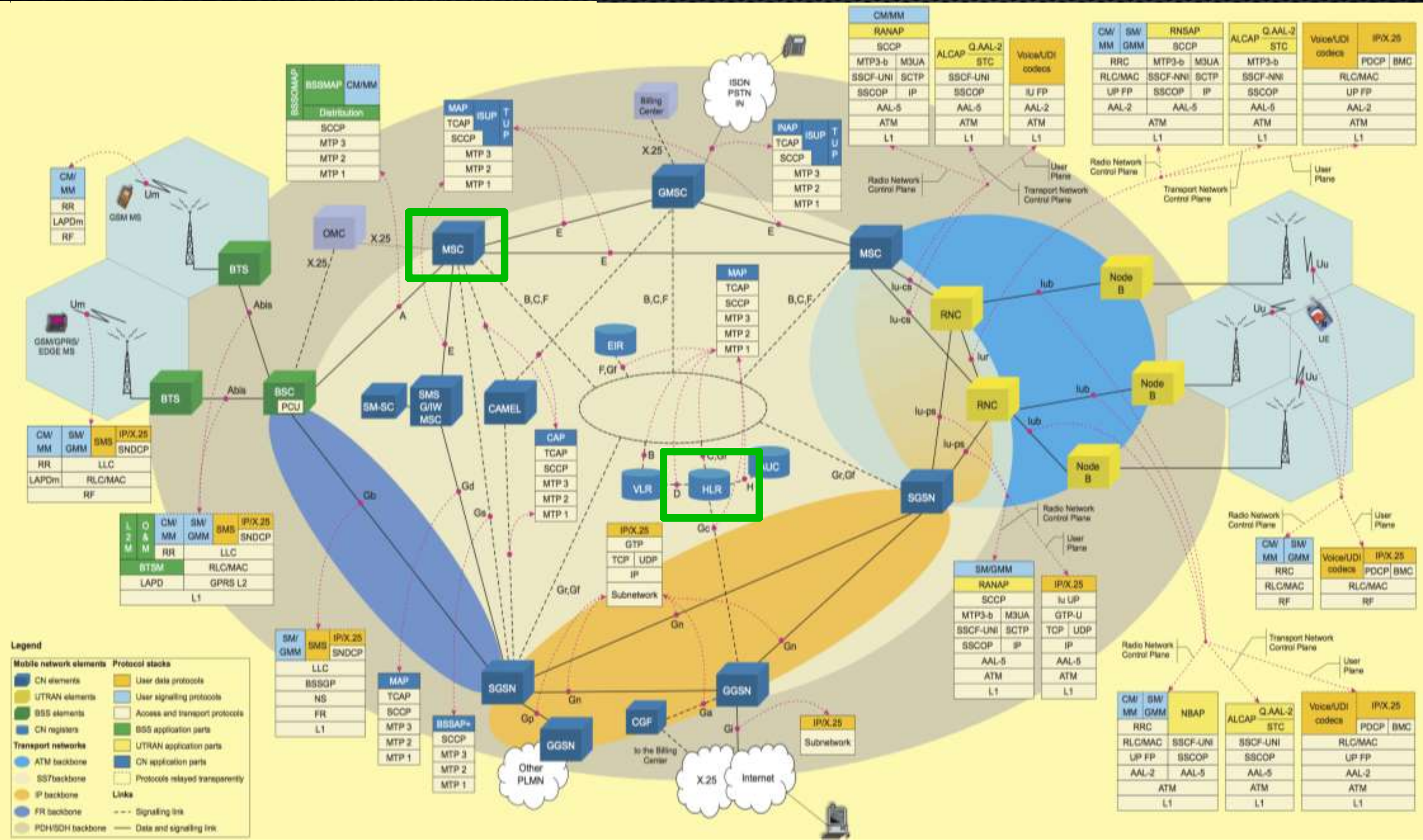
- Architecture diagrams for 2G / 3G
- Most important Network Elements
- SS7 stack and interconnections

Practical attack scenarios

- Mapping the SS7 network
- Tracking user location
- Sending spoofed SMS
- Demo

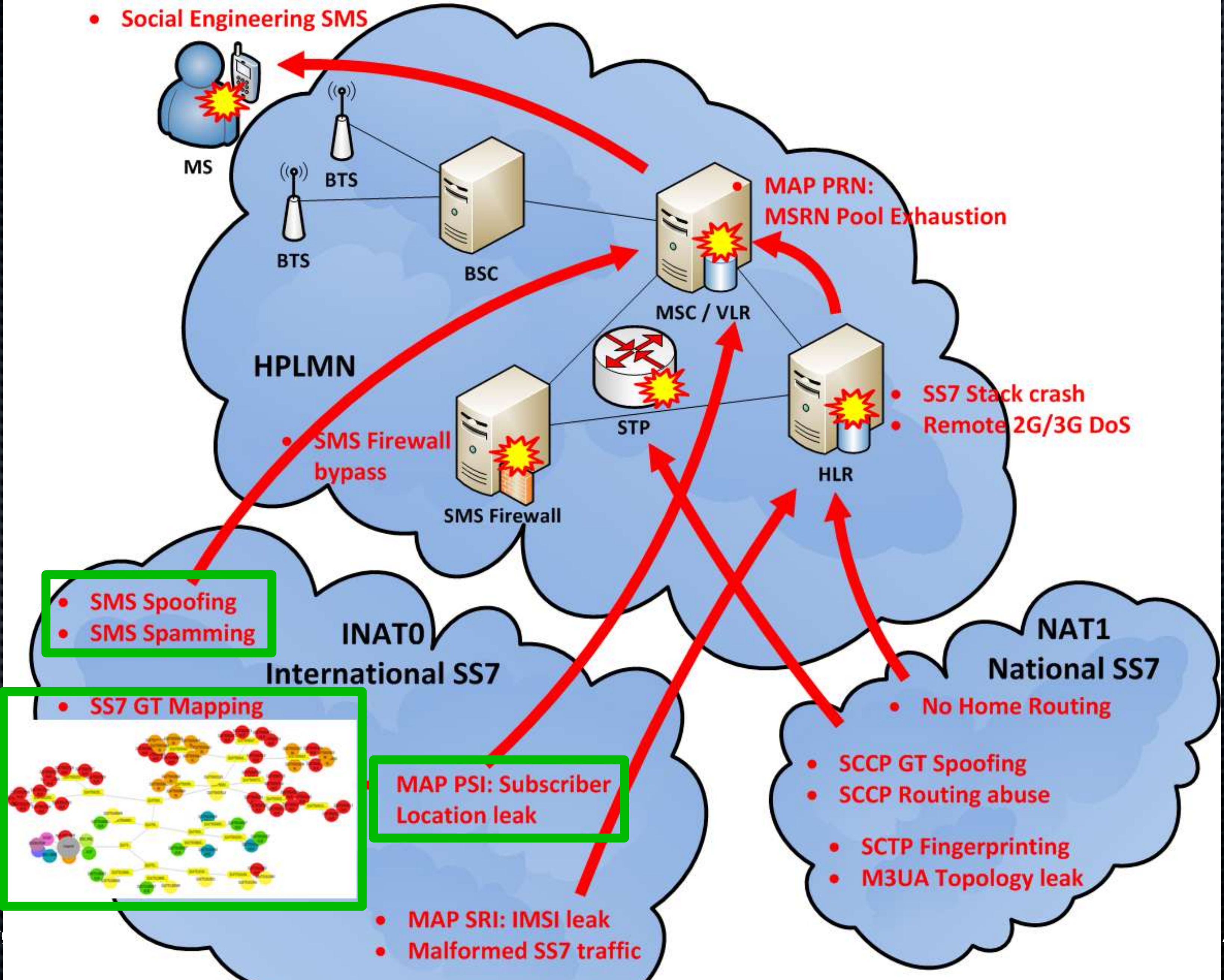
Telecom Overview

Evolution from 2G to 3G



Practical Attack Scenarios

SS7 Attack Vectors



Agenda

- Overall telecom architecture
  - Architecture diagrams for 2G / 3G
  - Most important Network Elements
  - SS7 stack and interconnections
- Practical attack scenarios
  - Mapping the SS7 network
  - Tracking user location
  - Sending spoofed SMS
  - Demo

MSC

Mobile Switching Center

- MSC: 5-50 per MNO
- Connected to 20-50 BSC
- In charge of call establishment
- Interfaces the BSC toward the rest of the network
- Connects the calls of the mobile users
- UE is attached to one MSC
- MAP Protocol
- Generates CDR (Charging Data Record)
- Security impact: Key compromise, content compromise, regional DoS, location tracking, …

Siemens MSC

HLR / HSS

Home Location Register
Home Subscriber Server

- HLR: 1-20 per MNO
- “Heart” of SS7 / SIGTRAN
- Subscriber database
  - IMSI
  - Authentication (AuC) : Ki
  - Current subscriber location
  - Supplementary services
- Queries from international partners (roaming)
- MAP Protocol
- Security impact: Key compromise, global DoS

NSN HLR / HSS

HLR / HSS

Home Location Register
Home Subscriber Server

- I’m Root !

Agenda

Overall telecom architecture

- Architecture diagrams for 2G / 3G
- Most important Network Elements
- SS7 stack and interconnections

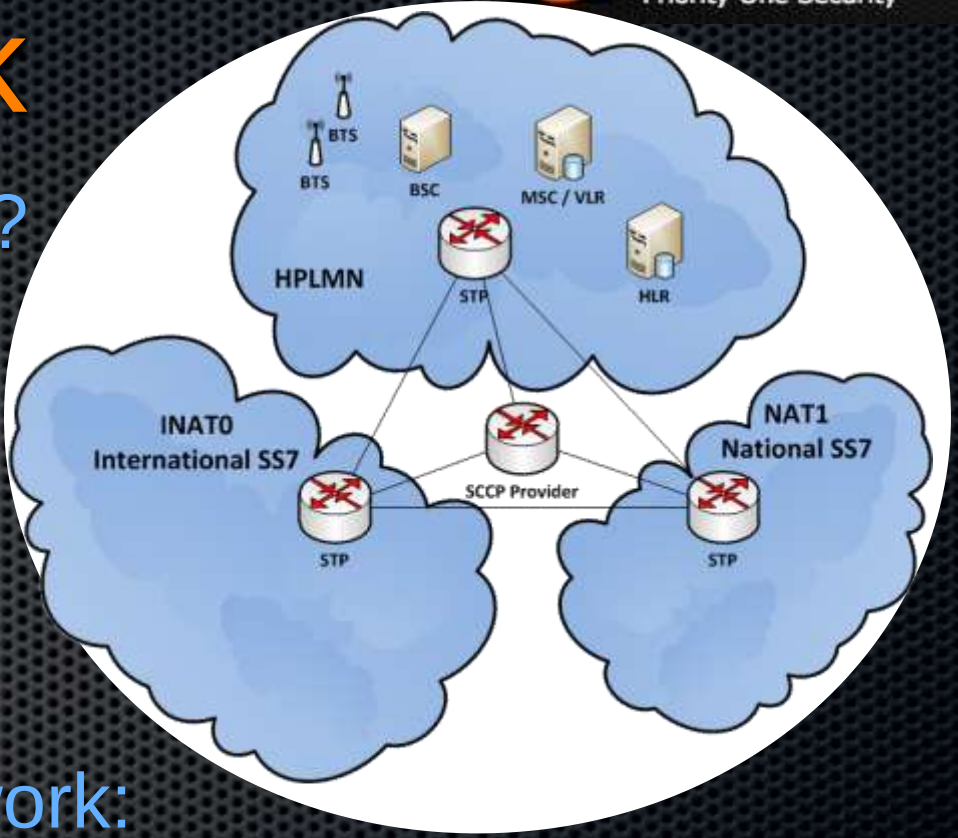
Practical attack scenarios

- Mapping the SS7 network
- Tracking user location
- Sending spoofed SMS
- Demo

Global SS7 network

- Private and secure SS7 network ?

- Interconnects many actors
- Different views depending on interconnection point

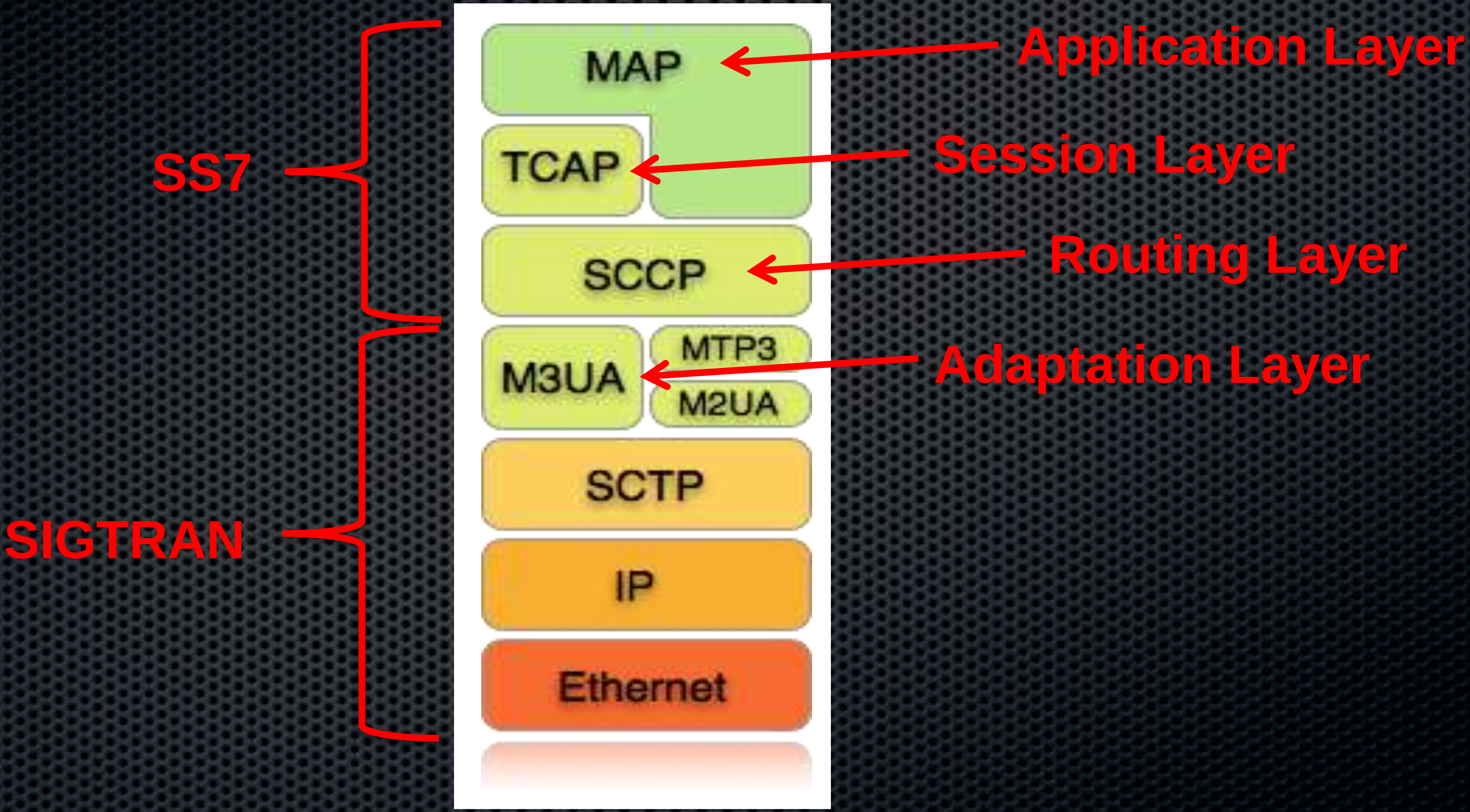


- Malicious entry point to SS7 network:
  - Through any unsecure operator and attack other operators from there
  - From Network Element OAM interface exposed on Internet
  - Through compromised Femto Cell
  - … and more …

P1 Security
Priority One Security

SS7 / SIGTRAN Stack

Protocol Layers



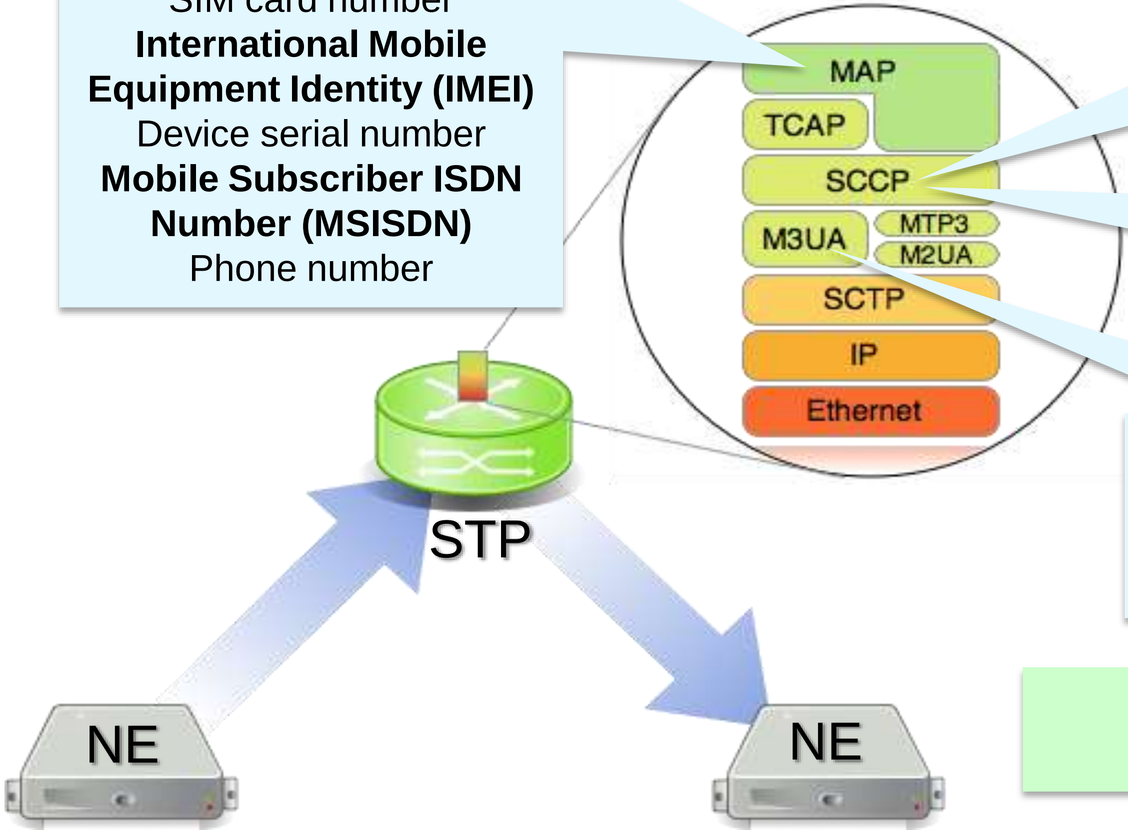
SIGTRAN MAP Stack

SS7 / SIGTRAN Stack

Addressing schemes

In Telecom networks a multitude of addressing schemes are used to identify Network Elements, subscribers, applications

International Mobile Subscriber Identity (IMSI)
SIM card number
International Mobile Equipment Identity (IMEI)
Device serial number
Mobile Subscriber ISDN Number (MSISDN)
Phone number



SubSystem Number (SSN)
Identifies application or service on Network Elements.
Equivalent to TCP port.

Global Title (GT)
Length up to 15 digits.
Looks like a phone number.
Equivalent to IP address.

Point Code (PC)
14 or 24 bits address.
Equivalent to MAC address.

SS7 Routing criteria:
PC / GT / SSN or combo

Agenda

- Overall telecom architecture
  - Architecture diagrams for 2G / 3G
  - Most important Network Elements
  - SS7 stack and interconnections
- Practical attack scenarios
  - Mapping the SS7 network
  - Tracking user location
  - Sending spoofed SMS
  - Demo

Practical Attack Scenarios

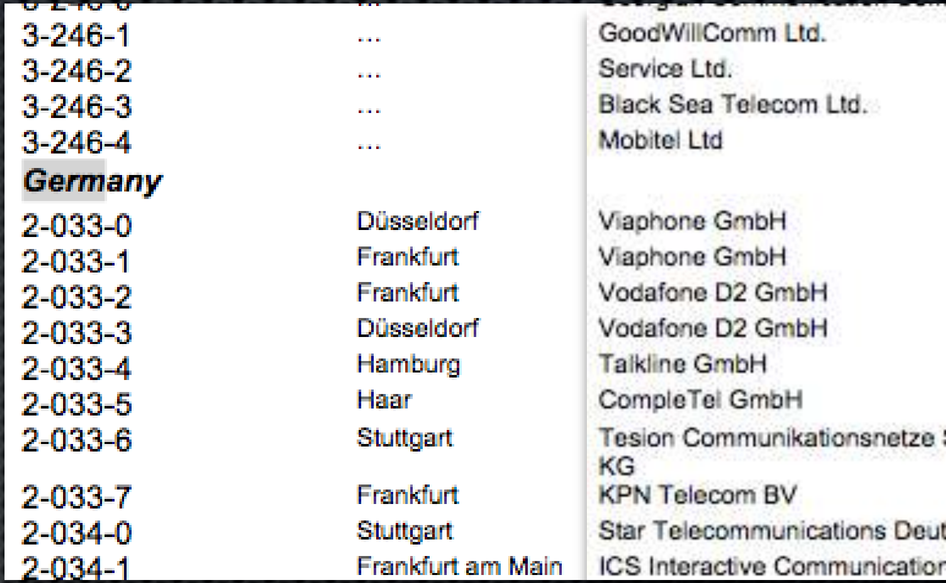
Scan methodology

- Abusing legitimate messages (SRISM, SRI, ATI, …)
- Sending from any international SS7 interconnection
- Steps:
  - Discovery scan and GT mapping: SCCP + TCAP
  - Advanced attacks: specific MAP messages
- Targets:
  - Attacking operators infrastructure
  - Attacking subscribers

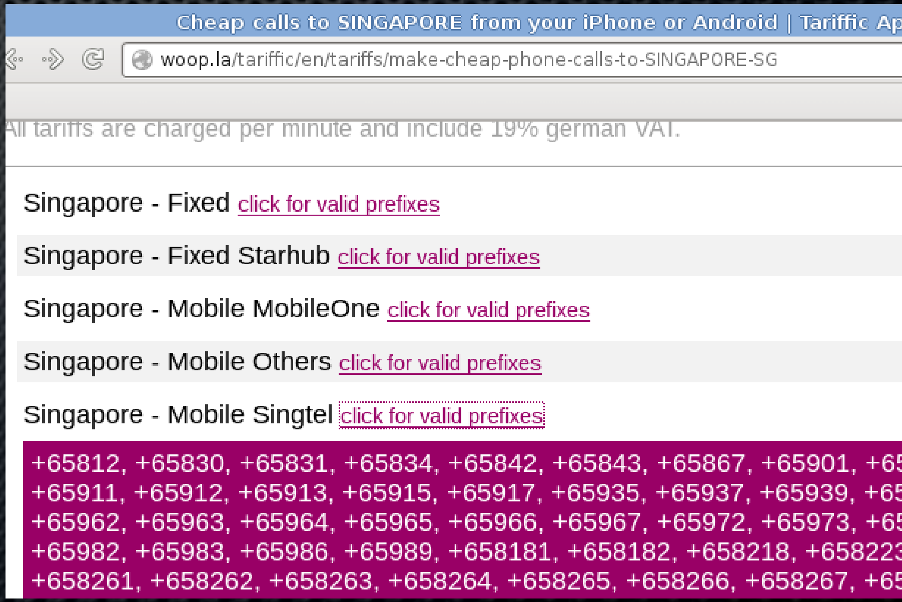
Discovery phase

Finding the first targets

- Publicly available information
  - International PC lists
  - GT prefix / country / operator
  - Subscriber MSISDN lists
- Probing from UE
  - SS codes: *#61#
  - Send SMS to your own SMSC to find your current MSC
- Changing GT prefix length
- Scan around confirmed targets



3-246-1	...	GoodWillComm Ltd.
3-246-2	...	Service Ltd.
3-246-3	...	Black Sea Telecom Ltd.
3-246-4	...	Mobitel Ltd
Germany		
2-033-0	Düsseldorf	Viaphone GmbH
2-033-1	Frankfurt	Viaphone GmbH
2-033-2	Frankfurt	Vodafone D2 GmbH
2-033-3	Düsseldorf	Vodafone D2 GmbH
2-033-4	Hamburg	Talkline GmbH
2-033-5	Haar	CompleTel GmbH
2-033-6	Stuttgart	Tesion Communikationsnetze KG
2-033-7	Frankfurt	KPN Telecom BV
2-034-0	Stuttgart	Star Telecommunications Deut
2-034-1	Frankfurt am Main	ICS Interactive Communicatior



Cheap calls to SINGAPORE from your iPhone or Android | Tariffic Ap

woop.la/tariffic/en/tariffs/make-cheap-phone-calls-to-SINGAPORE-SG

All tariffs are charged per minute and include 19% german VAT.

Singapore - Fixed click for valid prefixes

Singapore - Fixed Starhub click for valid prefixes

Singapore - Mobile MobileOne click for valid prefixes

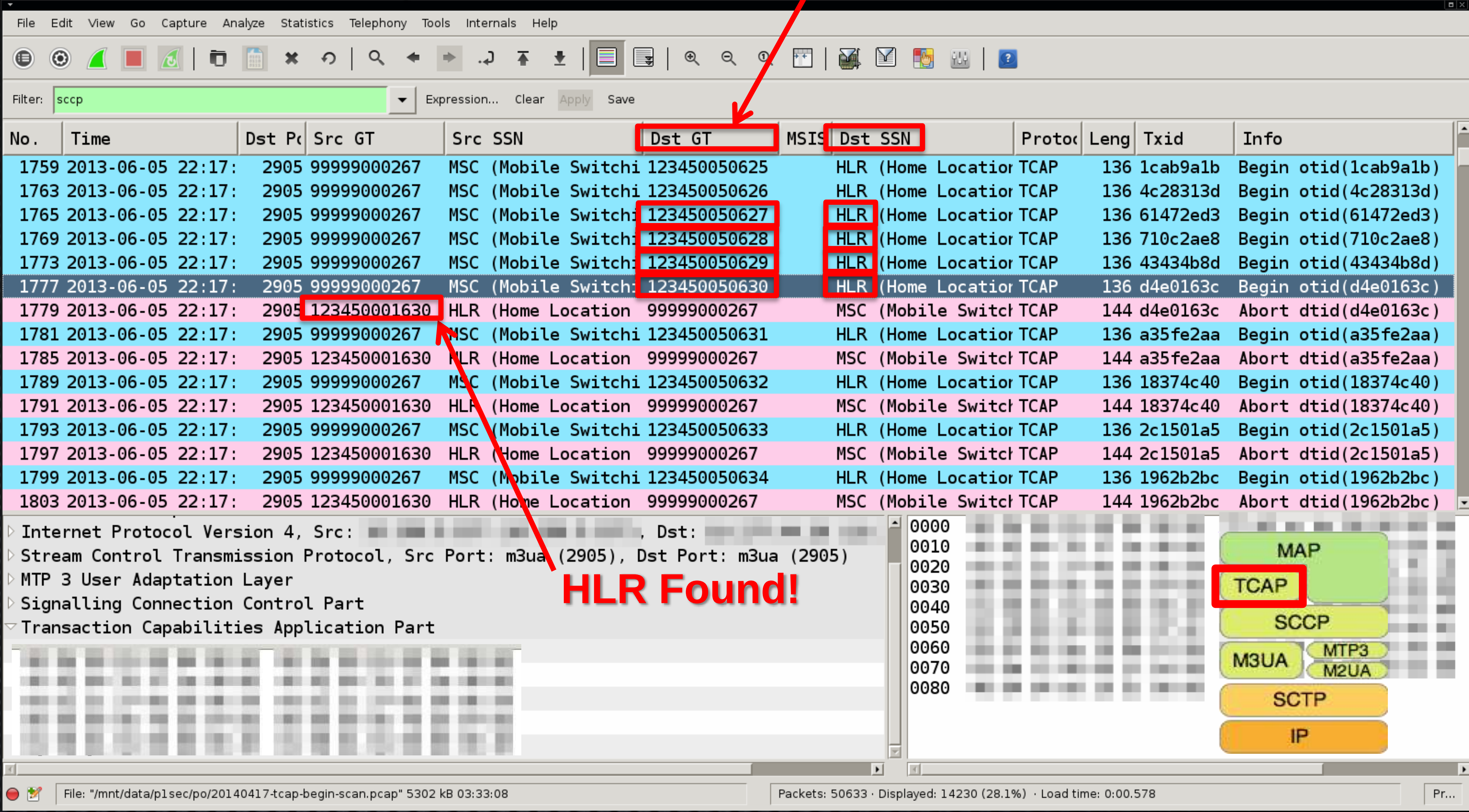
Singapore - Mobile Others click for valid prefixes

Singapore - Mobile Singtel click for valid prefixes

+65812, +65830, +65831, +65834, +65842, +65843, +65867, +65901, +65
+65911, +65912, +65913, +65915, +65917, +65935, +65937, +65939, +65
+65962, +65963, +65964, +65965, +65966, +65967, +65972, +65973, +65
+65982, +65983, +65986, +65989, +658181, +658182, +658218, +658223
+658261, +658262, +658263, +658264, +658265, +658266, +658267, +65

Discovery phase

TCAP scan example



Filter: sccp

No.	Time	Dst Pc	Src GT	Src SSN	Dst GT	MSIS	Dst SSN	Protoc	Leng	Txid	Info
1759	2013-06-05 22:17:	2905	99999000267	MSC (Mobile Switchi	123450050625		HLR (Home Locatior	TCAP	136	1cab9a1b	Begin otid(1cab9a1b)
1763	2013-06-05 22:17:	2905	99999000267	MSC (Mobile Switchi	123450050626		HLR (Home Locatior	TCAP	136	4c28313d	Begin otid(4c28313d)
1765	2013-06-05 22:17:	2905	99999000267	MSC (Mobile Switchi	123450050627		HLR (Home Locatior	TCAP	136	61472ed3	Begin otid(61472ed3)
1769	2013-06-05 22:17:	2905	99999000267	MSC (Mobile Switchi	123450050628		HLR (Home Locatior	TCAP	136	710c2ae8	Begin otid(710c2ae8)
1773	2013-06-05 22:17:	2905	99999000267	MSC (Mobile Switchi	123450050629		HLR (Home Locatior	TCAP	136	43434b8d	Begin otid(43434b8d)
1777	2013-06-05 22:17:	2905	99999000267	MSC (Mobile Switchi	123450050630		HLR (Home Locatior	TCAP	136	d4e0163c	Begin otid(d4e0163c)
1779	2013-06-05 22:17:	2905	123450001630	HLR (Home Location	99999000267		MSC (Mobile Switcl	TCAP	144	d4e0163c	Abort dtid(d4e0163c)
1781	2013-06-05 22:17:	2905	99999000267	MSC (Mobile Switchi	123450050631		HLR (Home Locatior	TCAP	136	a35fe2aa	Begin otid(a35fe2aa)
1785	2013-06-05 22:17:	2905	123450001630	HLR (Home Location	99999000267		MSC (Mobile Switcl	TCAP	144	a35fe2aa	Abort dtid(a35fe2aa)
1789	2013-06-05 22:17:	2905	99999000267	MSC (Mobile Switchi	123450050632		HLR (Home Locatior	TCAP	136	18374c40	Begin otid(18374c40)
1791	2013-06-05 22:17:	2905	123450001630	HLR (Home Location	99999000267		MSC (Mobile Switcl	TCAP	144	18374c40	Abort dtid(18374c40)
1793	2013-06-05 22:17:	2905	99999000267	MSC (Mobile Switchi	123450050633		HLR (Home Locatior	TCAP	136	2c1501a5	Begin otid(2c1501a5)
1797	2013-06-05 22:17:	2905	123450001630	HLR (Home Location	99999000267		MSC (Mobile Switcl	TCAP	144	2c1501a5	Abort dtid(2c1501a5)
1799	2013-06-05 22:17:	2905	99999000267	MSC (Mobile Switchi	123450050634		HLR (Home Locatior	TCAP	136	1962b2bc	Begin otid(1962b2bc)
1803	2013-06-05 22:17:	2905	123450001630	HLR (Home Location	99999000267		MSC (Mobile Switcl	TCAP	144	1962b2bc	Abort dtid(1962b2bc)

```
▷ Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
▷ Stream Control Transmission Protocol, Src Port: m3ua (2905), Dst Port: m3ua (2905)
▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
▽ Transaction Capabilities Application Part
[redacted]
```

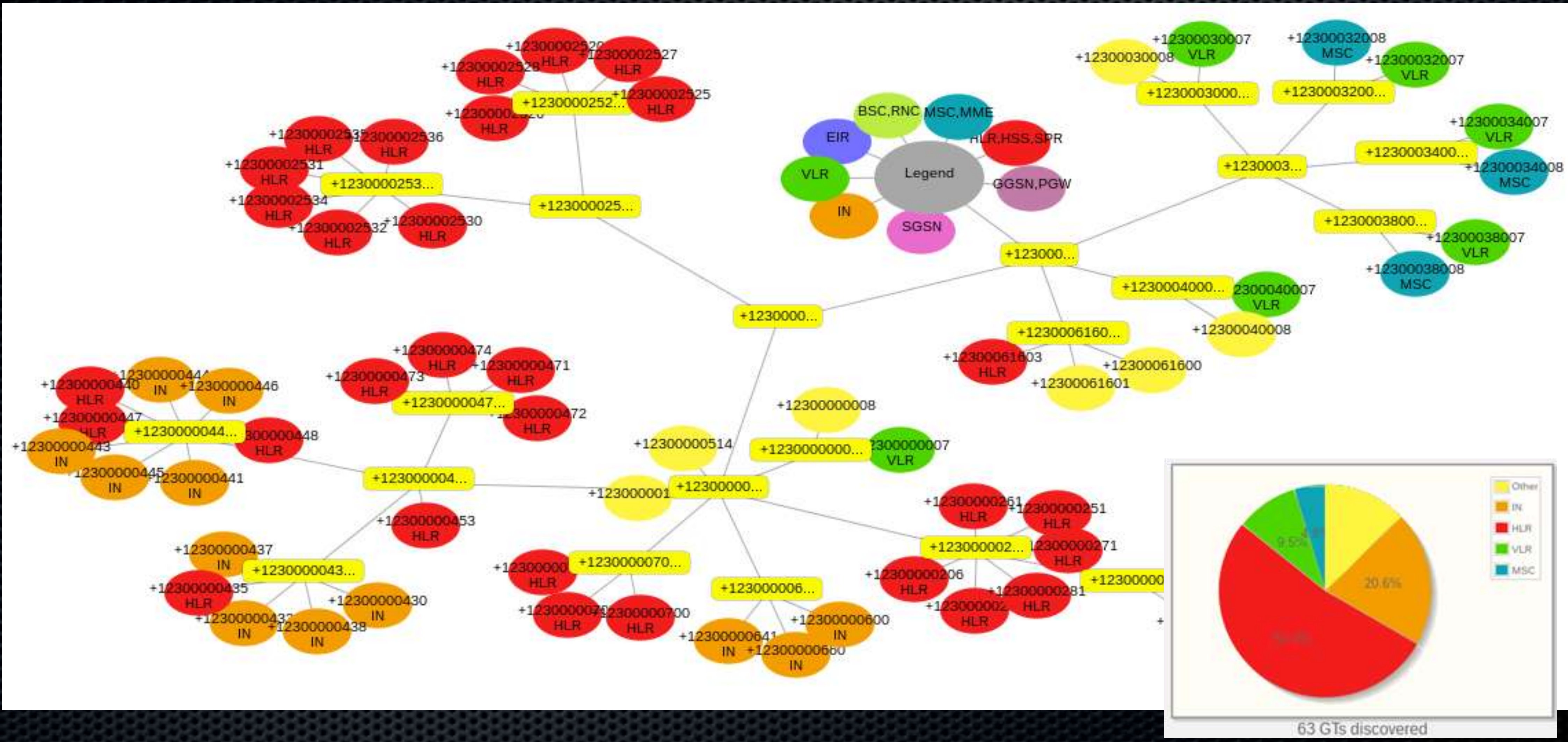
```
0000 [redacted]
0010
0020
0030
0040
0050
0060
0070
0080
```

File: "/mnt/data/p1sec/po/20140417-tcap-begin-scan.pcap" 5302 kB 03:33:08

Packets: 50633 · Displayed: 14230 (28.1%) · Load time: 0:00.578

2G / 3G Network Mapping

Active Network Mapping



Agenda

Overall telecom architecture

- Architecture diagrams for 2G / 3G
- Most important Network Elements
- SS7 stack and interconnections

Practical attack scenarios

- Mapping the SS7 network
- Tracking user location
- Sending spoofed SMS
- Demo

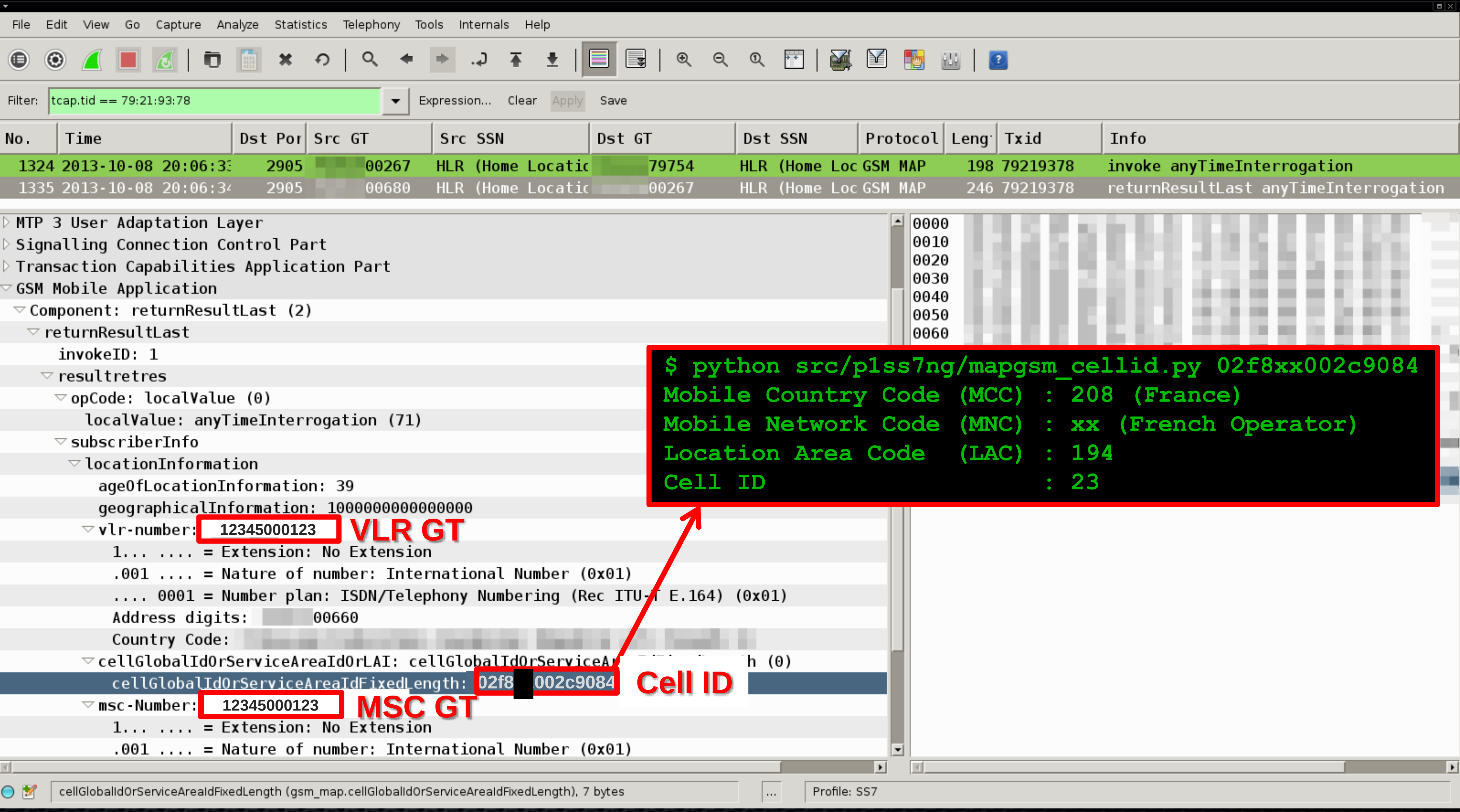
Spying on users

Tracking user location

- Based on non filtered MAP messages
  - SRISM / SRI
  - PSI / PSL
  - ATI ….
- Targeted towards HLR or MSC / VLR
- Accuracy:
  - Depending on type of message allowed
  - MSC GT (Accuracy: City / Region)
  - CellID (Accuracy: Street)

Tracking user location

Get MSC / VLR / CellID from SS7 (Example with MAP ATI)



Filter: tcap.tid == 79:21:93:78

No.	Time	Dst Por	Src GT	Src SSN	Dst GT	Dst SSN	Protocol	Leng	Txid	Info
1324	2013-10-08 20:06:3:	2905	[redacted]00267	HLR (Home Locatic	[redacted]79754	HLR (Home Loc	GSM MAP	198	79219378	invoke anyTimeInterrogation
1335	2013-10-08 20:06:3‹	2905	[redacted]00680	HLR (Home Locatic	[redacted]00267	HLR (Home Loc	GSM MAP	246	79219378	returnResultLast anyTimeInterrogation

```
▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
▽ GSM Mobile Application
  ▽ Component: returnResultLast (2)
    ▽ returnResultLast
        invokeID: 1
      ▽ resultretres
        ▽ opCode: localValue (0)
            localValue: anyTimeInterrogation (71)
        ▽ subscriberInfo
          ▽ locationInformation
              ageOfLocationInformation: 39
              geographicalInformation: 1000000000000000
            ▽ vlr-number: 12345000123
                1... .... = Extension: No Extension
                .001 .... = Nature of number: International Number (0x01)
                .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x01)
                Address digits: [redacted]00660
                Country Code: [redacted]
            ▽ cellGlobalIdOrServiceAreaIdOrLAI: cellGlobalIdOrServiceA... ...h (0)
                cellGlobalIdOrServiceAreaIdFixedLength: 02f8[redacted]002c9084
            ▽ msc-Number: 12345000123
                1... .... = Extension: No Extension
                .001 .... = Nature of number: International Number (0x01)
```

```
0000 [redacted]
0010
0020
0030
0040
0050
0060
```

VLR GT

Cell ID

MSC GT

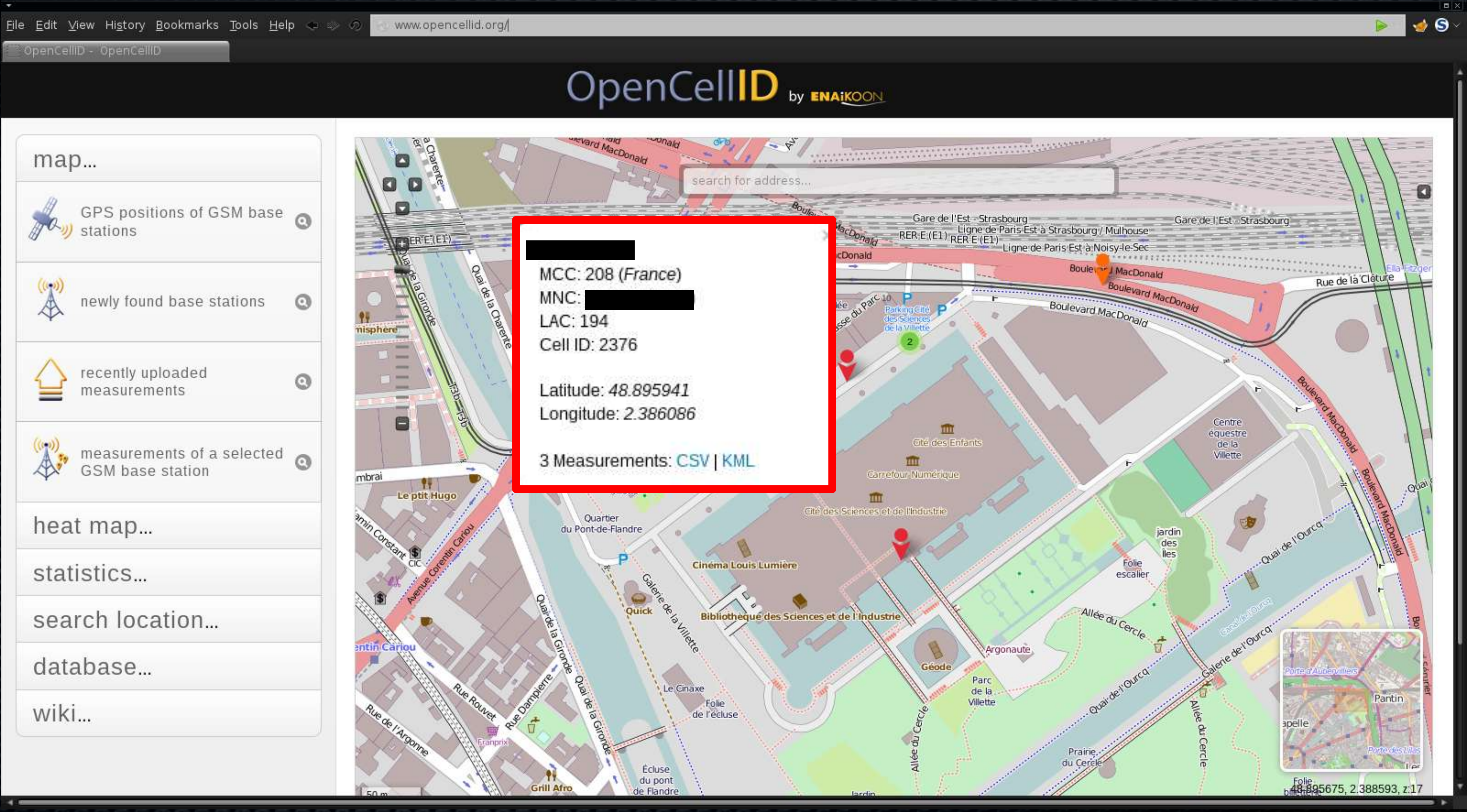
```
$ python src/p1ss7ng/mapgsm_cellid.py 02f8xx002c9084
Mobile Country Code (MCC)  : 208 (France)
Mobile Network Code (MNC)  : xx (French Operator)
Location Area Code  (LAC)  : 194
Cell ID                    : 23
```

cellGlobalIdOrServiceAreaIdFixedLength (gsm_map.cellGlobalIdOrServiceAreaIdFixedLength), 7 bytes

Profile: SS7

Tracking user location

Open CellID databases


File Edit View History Bookmarks Tools Help
www.opencellid.org/
OpenCellID - OpenCellID
OpenCellID by ENAiKOON
map...
GPS positions of GSM base stations
newly found base stations
recently uploaded measurements
measurements of a selected GSM base station
heat map...
statistics...
search location...
database...
wiki...
search for address...
Gare de l'Est - Strasbourg
Boulevard MacDonald
Cité des Sciences et de l'Industrie
Cinéma Louis Lumière
Bibliothèque des Sciences et de l'Industrie
Géode
Parc de la Villette
Quai de l'Ourcq
48.895675, 2.388593, z:17

[redacted]

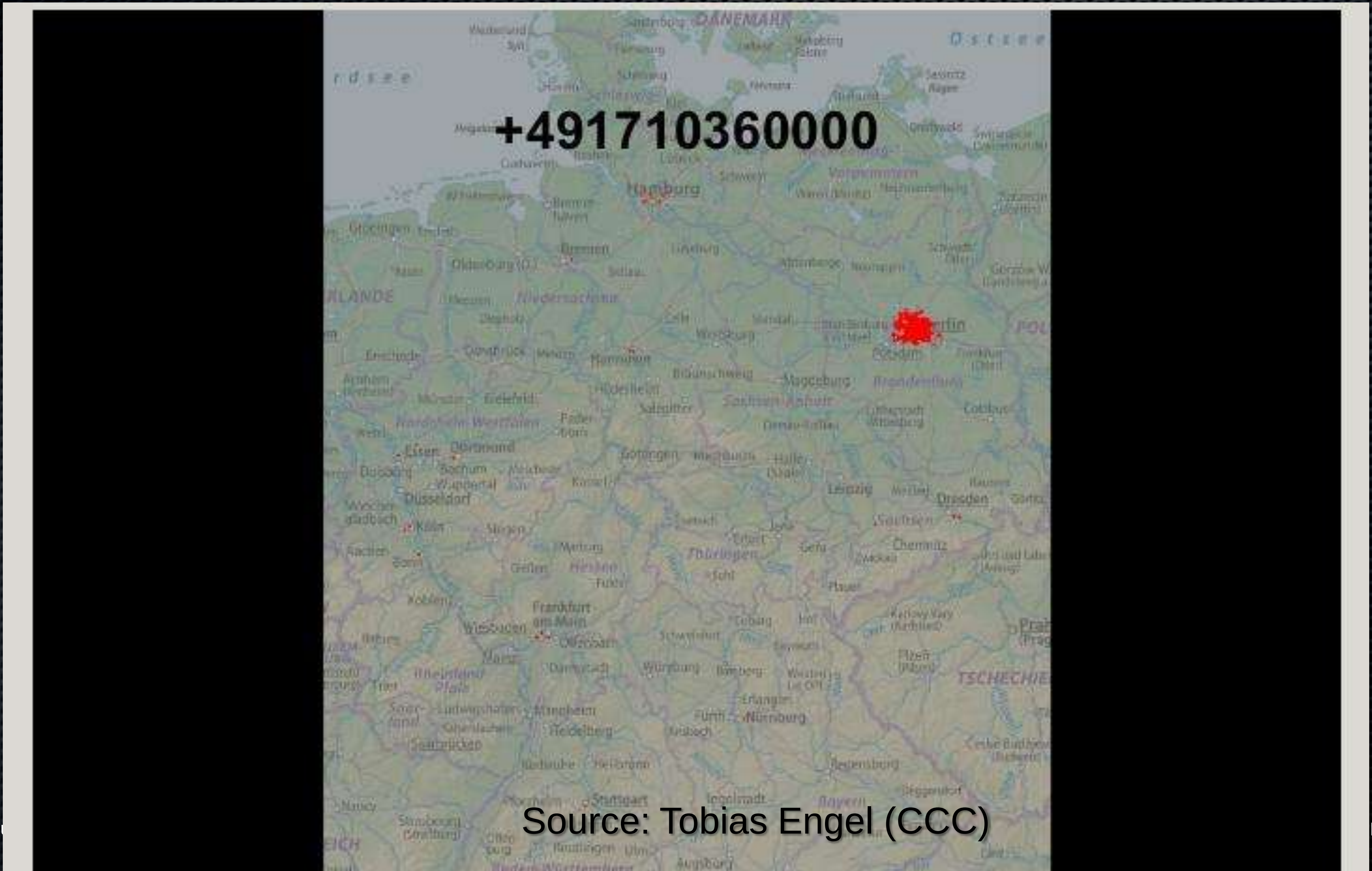
MCC: 208 (*France*)
MNC: [redacted]
LAC: 194
Cell ID: 2376

Latitude: *48.895941*
Longitude: *2.386086*

3 Measurements: CSV | KML

Tracking user location

Low accuracy (MSC based location)



Source: Tobias Engel (CCC)

Agenda

Overall telecom architecture

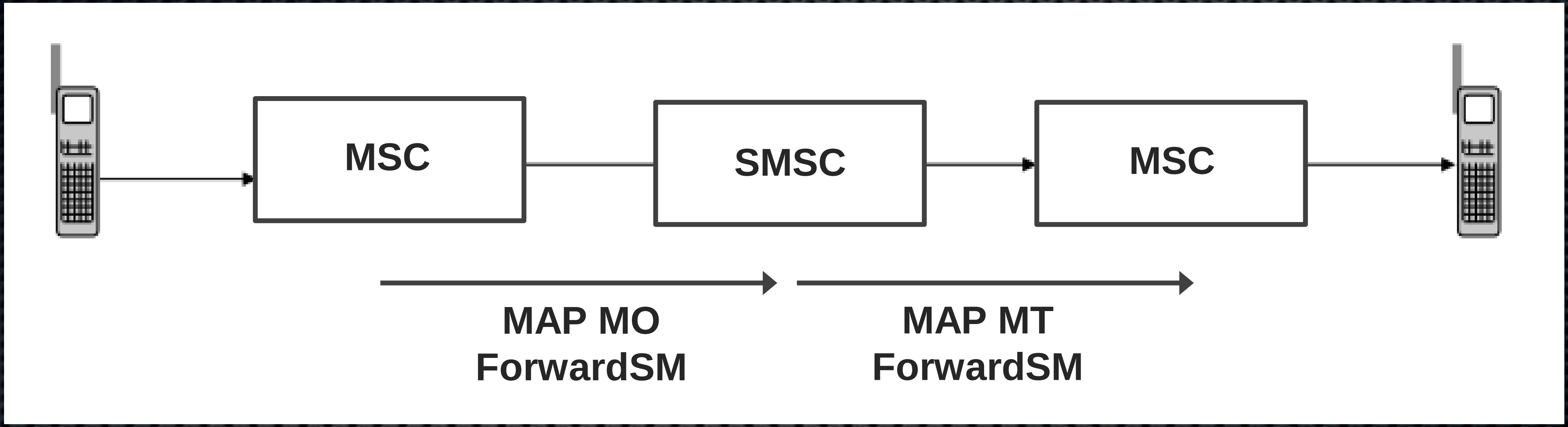
- Architecture diagrams for 2G / 3G
- Most important Network Elements
- SS7 stack and interconnections

Practical attack scenarios

- Mapping the SS7 network
- Tracking user location
- Sending spoofed SMS
- Demo

Sending SMS

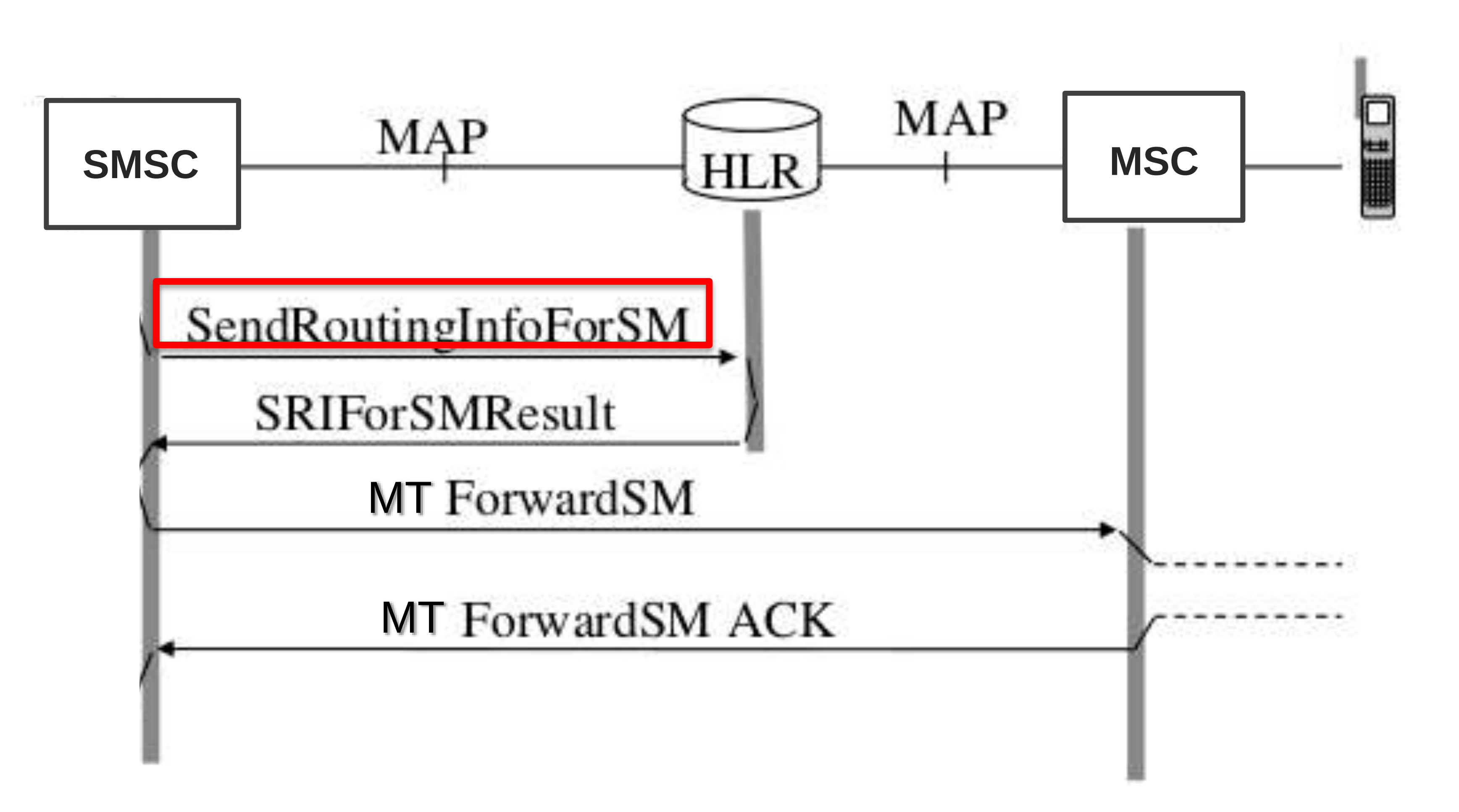
MO / MT ForwardSM



- MAP messages
- MO: Mobile Originating
- MT: Mobile Terminating
- SMSC: SMS Center (SMSC GT list is public)

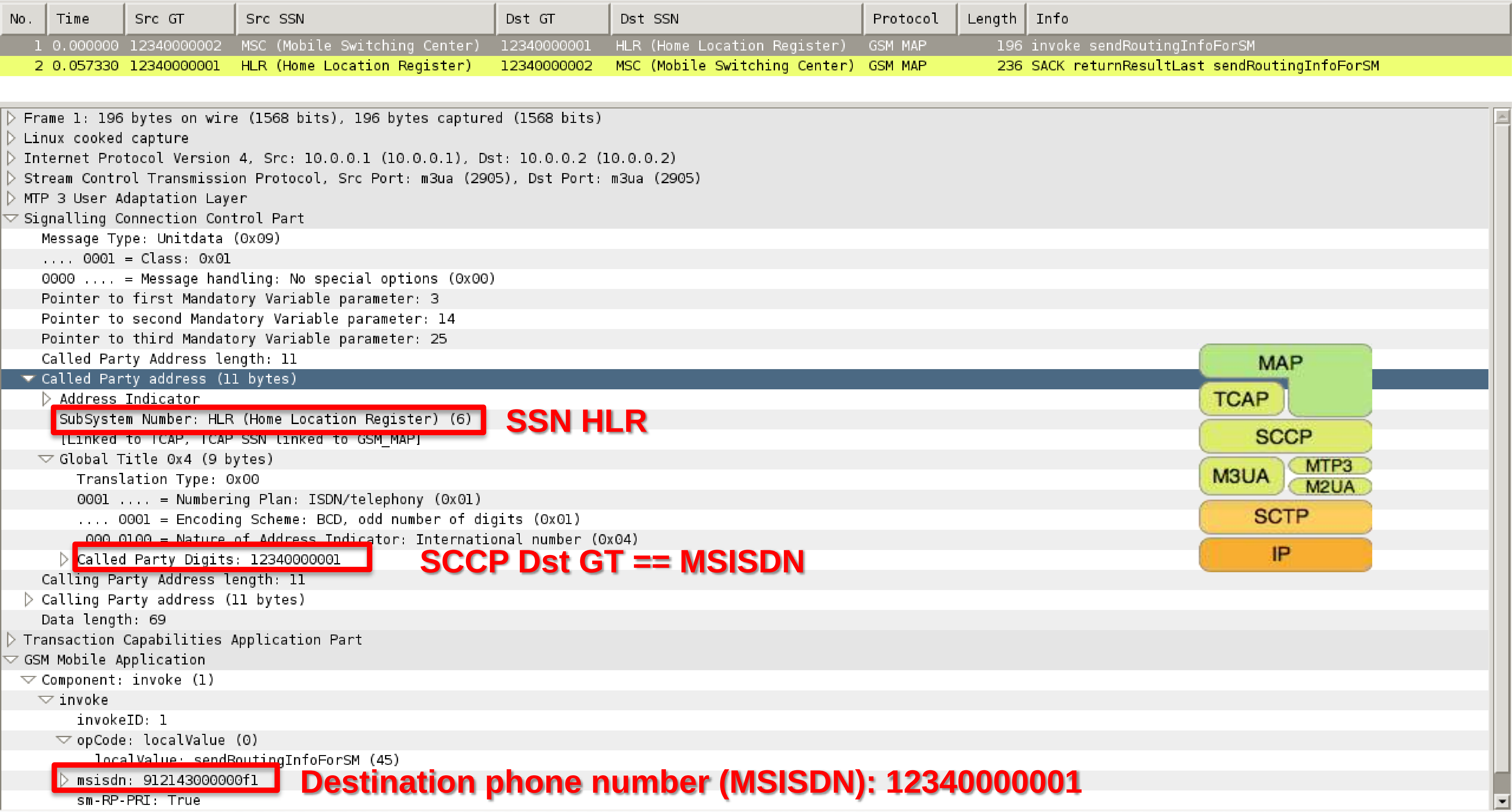
Sending SMS

Prerequisite to SMS: MAP SRISM



SendRoutingInfoForSM

SS7 MAP SRISM



No.	Time	Src GT	Src SSN	Dst GT	Dst SSN	Protocol	Length	Info
1	0.000000	12340000002	MSC (Mobile Switching Center)	12340000001	HLR (Home Location Register)	GSM MAP	196	invoke sendRoutingInfoForSM
2	0.057330	12340000001	HLR (Home Location Register)	12340000002	MSC (Mobile Switching Center)	GSM MAP	236	SACK returnResultLast sendRoutingInfoForSM

```
▷ Frame 1: 196 bytes on wire (1568 bits), 196 bytes captured (1568 bits)
▷ Linux cooked capture
▷ Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.2 (10.0.0.2)
▷ Stream Control Transmission Protocol, Src Port: m3ua (2905), Dst Port: m3ua (2905)
▷ MTP 3 User Adaptation Layer
▽ Signalling Connection Control Part
    Message Type: Unitdata (0x09)
    .... 0001 = Class: 0x01
    0000 .... = Message handling: No special options (0x00)
    Pointer to first Mandatory Variable parameter: 3
    Pointer to second Mandatory Variable parameter: 14
    Pointer to third Mandatory Variable parameter: 25
    Called Party Address length: 11
  ▼ Called Party address (11 bytes)
    ▷ Address Indicator
      SubSystem Number: HLR (Home Location Register) (6)
      [Linked to TCAP, TCAP SSN linked to GSM_MAP]
    ▽ Global Title 0x4 (9 bytes)
        Translation Type: 0x00
        0001 .... = Numbering Plan: ISDN/telephony (0x01)
        .... 0001 = Encoding Scheme: BCD, odd number of digits (0x01)
        .000 0100 = Nature of Address Indicator: International number (0x04)
      ▷ Called Party Digits: 12340000001
    Calling Party Address length: 11
  ▷ Calling Party address (11 bytes)
    Data length: 69
▷ Transaction Capabilities Application Part
▽ GSM Mobile Application
  ▽ Component: invoke (1)
    ▽ invoke
        invokeID: 1
      ▽ opCode: localValue (0)
          localValue: sendRoutingInfoForSM (45)
      ▷ msisdn: 912143000000f1
        sm-RP-PRI: True
```

SSN HLR

SCCP Dst GT == MSISDN

Destination phone number (MSISDN): 12340000001

Answer to SRISM

Answer comes from HLR

Get IMSI for requested MSISDN

```
RoutingInfoForSM-Res ::= SEQUENCE {
     imsi                    IMSI,
     locationInfoWithLMSI[0] LocationInfoWithLMSI,
     extensionContainer    [4] ExtensionContainer
     OPTIONAL,
     ...,
     ip-sm-gwGuidance      [5] IP-SM-GW-Guidance
     OPTIONAL }
```

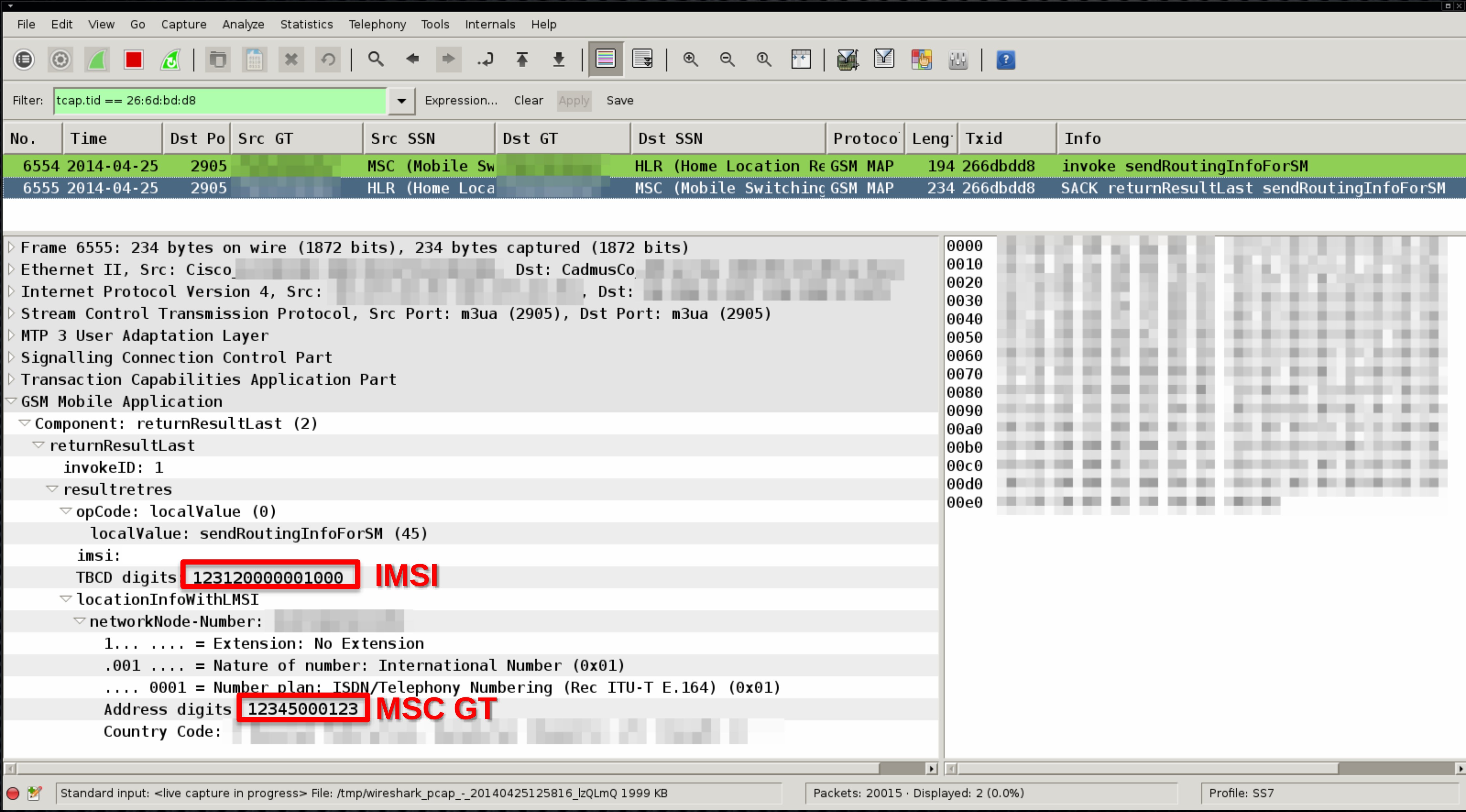
Contains MSC GT

- Both IMSI and MSC GT are required to send MAP MT Forward SM

P1 Security
Priority One Security

Answer to SRISM

SRISM answer reveals MSC GT and IMSI



Filter: tcap.tid == 26:6d:bd:d8

No.	Time	Dst Po	Src GT	Src SSN	Dst GT	Dst SSN	Protoco	Leng	Txid	Info
6554	2014-04-25	2905	[redacted]	MSC (Mobile Sw	[redacted]	HLR (Home Location Re	GSM MAP	194	266dbdd8	invoke sendRoutingInfoForSM
6555	2014-04-25	2905	[redacted]	HLR (Home Loca	[redacted]	MSC (Mobile Switching	GSM MAP	234	266dbdd8	SACK returnResultLast sendRoutingInfoForSM

```
▷ Frame 6555: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits)
▷ Ethernet II, Src: Cisco_[redacted] Dst: CadmusCo_[redacted]
▷ Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
▷ Stream Control Transmission Protocol, Src Port: m3ua (2905), Dst Port: m3ua (2905)
▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
▽ GSM Mobile Application
  ▽ Component: returnResultLast (2)
    ▽ returnResultLast
        invokeID: 1
      ▽ resultretres
        ▽ opCode: localValue (0)
            localValue: sendRoutingInfoForSM (45)
          imsi:
         TBCD digits: 123120000001000
        ▽ locationInfoWithLMSI
          ▽ networkNode-Number: [redacted]
              1... .... = Extension: No Extension
              .001 .... = Nature of number: International Number (0x01)
              .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x01)
              Address digits: 12345000123
              Country Code: [redacted]
```

```
0000 [redacted]
0010
0020
0030
0040
0050
0060
0070
0080
0090
00a0
00b0
00c0
00d0
00e0
```

Standard input: <live capture in progress> File: /tmp/wireshark_pcap_-_20140425125816_lzQLmQ 1999 KB

Packets: 20015 · Displayed: 2 (0.0%)

Profile: SS7

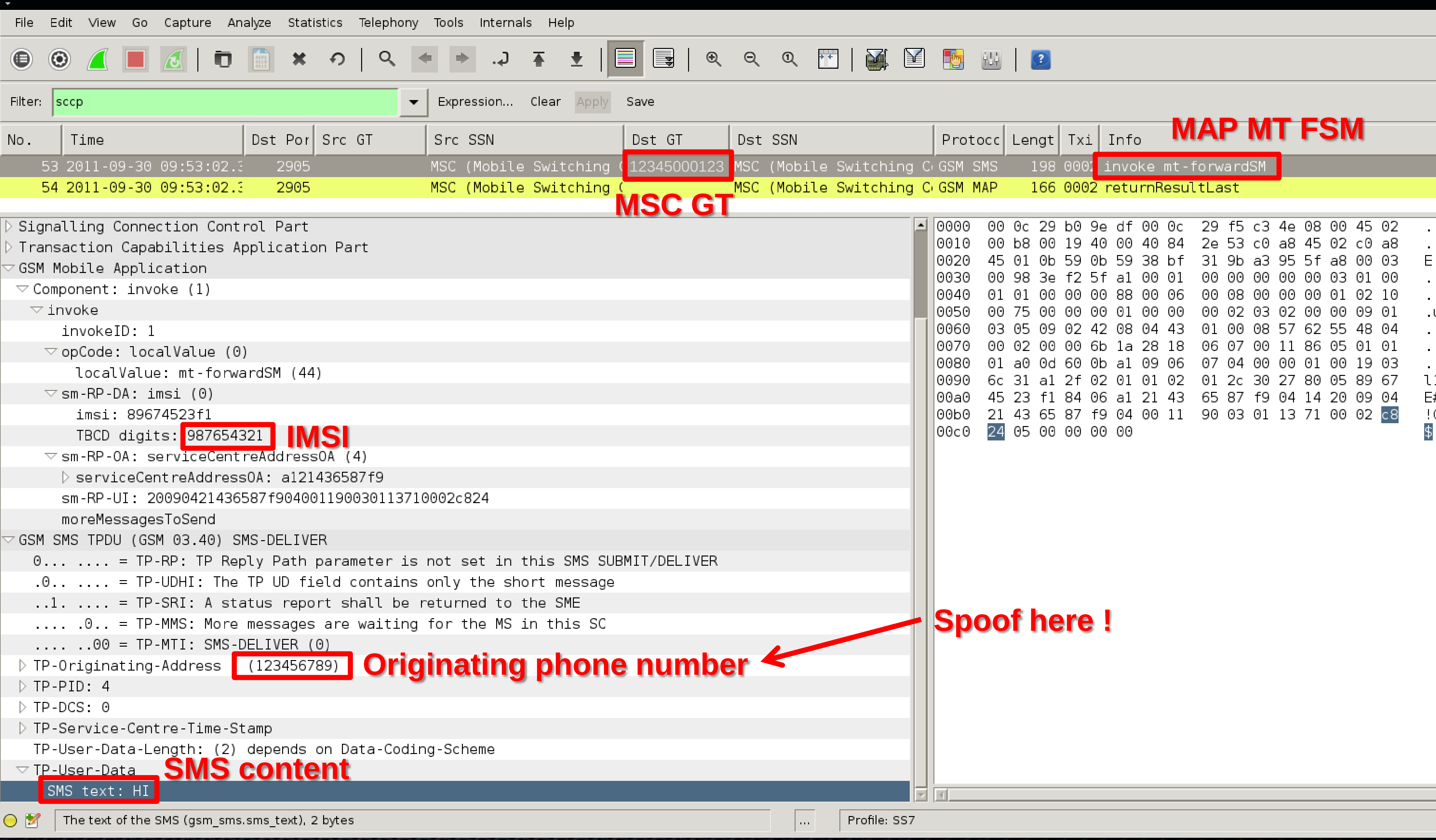
SMS attacks

- Sending spam SMS
- Sending spoof SMS
- Bypassing SMS firewall
  - Anti Spam protections
  - MT FSM directly targeting MSC
- Directly sent from signalling protocol

SMS attacks

P1 Security
Priority One Security

Based on MAP MT-FSM (Mobile Terminated Forward Short Message)


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Save

Filter: sccp

No.	Time	Dst Por	Src GT	Src SSN	Dst GT	Dst SSN	Protocc	Lengt	Txi	Info
53	2011-09-30 09:53:02.3	2905		MSC (Mobile Switching (	12345000123	MSC (Mobile Switching C	GSM SMS	198	0002	invoke mt-forwardSM
54	2011-09-30 09:53:02.3	2905		MSC (Mobile Switching (		MSC (Mobile Switching C	GSM MAP	166	0002	returnResultLast

MAP MT FSM

MSC GT

```
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
▽ GSM Mobile Application
  ▽ Component: invoke (1)
    ▽ invoke
        invokeID: 1
      ▽ opCode: localValue (0)
          localValue: mt-forwardSM (44)
      ▽ sm-RP-DA: imsi (0)
          imsi: 89674523f1
          TBCD digits: 987654321
      ▽ sm-RP-OA: serviceCentreAddressOA (4)
        ▷ serviceCentreAddressOA: a1214365 87f9
        sm-RP-UI: 20090421436587f904001190030113710002c824
        moreMessagesToSend
▽ GSM SMS TPDU (GSM 03.40) SMS-DELIVER
    0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
    .0.. .... = TP-UDHI: The TP UD field contains only the short message
    ..1. .... = TP-SRI: A status report shall be returned to the SME
    .... .0.. = TP-MMS: More messages are waiting for the MS in this SC
    .... ..00 = TP-MTI: SMS-DELIVER (0)
  ▷ TP-Originating-Address  (123456789)
  ▷ TP-PID: 4
  ▷ TP-DCS: 0
  ▷ TP-Service-Centre-Time-Stamp
    TP-User-Data-Length: (2) depends on Data-Coding-Scheme
  ▽ TP-User-Data
      SMS text: HI
```

IMSI

Originating phone number

Spoof here !

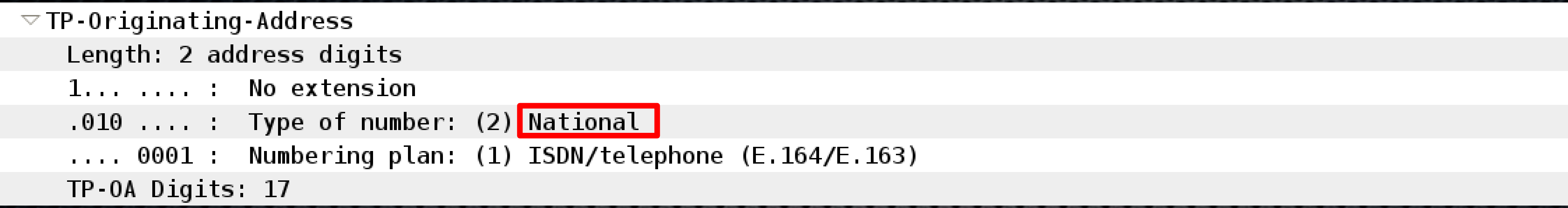
SMS content

```
0000  00 0c 29 b0 9e df 00 0c  29 f5 c3 4e 08 00 45 02   .
0010  00 b8 00 19 40 00 40 84  2e 53 c0 a8 45 02 c0 a8   .
0020  45 01 0b 59 0b 59 38 bf  31 9b a3 95 5f a8 00 03   E
0030  00 98 3e f2 5f a1 00 01  00 00 00 00 00 03 01 00   .
0040  01 01 00 00 00 88 00 06  00 08 00 00 00 01 02 10   .
0050  00 75 00 00 00 01 00 00  00 02 03 02 00 00 09 01   .u
0060  03 05 09 02 42 08 04 43  01 00 08 57 62 55 48 04   .
0070  00 02 00 00 6b 1a 28 18  06 07 00 11 86 05 01 01   .
0080  01 a0 0d 60 0b a1 09 06  07 04 00 00 01 00 19 03   .
0090  6c 31 a1 2f 02 01 01 02  01 2c 30 27 80 05 89 67   l1
00a0  45 23 f1 84 06 a1 21 43  65 87 f9 04 14 20 09 04   E#
00b0  21 43 65 87 f9 04 00 11  90 03 01 13 71 00 02 c8   !(
00c0  24 05 00 00 00 00                                  $
```

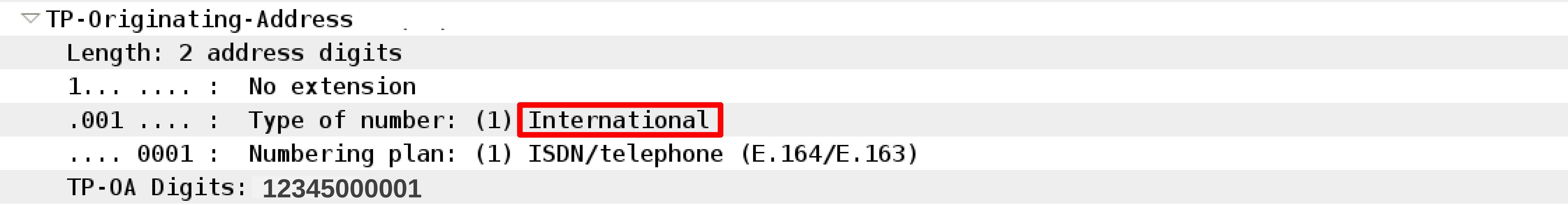
The text of the SMS (gsm_sms.sms_text), 2 bytes ... Profile: SS7

Originating Address

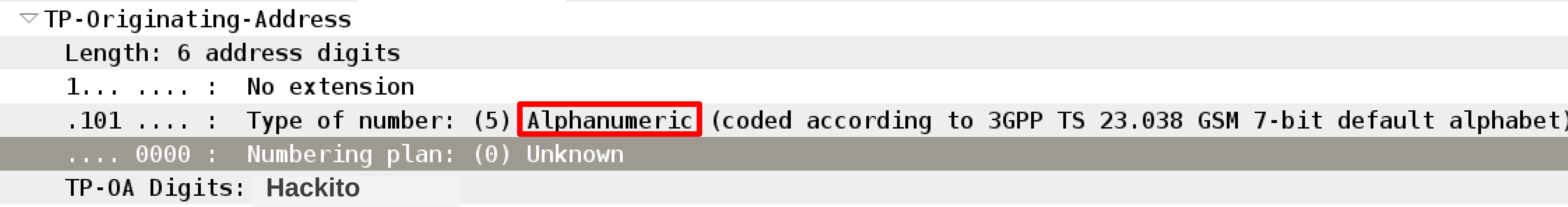
Try different encodings ! (Different screening rules)



```
▽ TP-Originating-Address
    Length: 2 address digits
    1... .... :  No extension
    .010 .... :  Type of number: (2) National
    .... 0001 :  Numbering plan: (1) ISDN/telephone (E.164/E.163)
    TP-OA Digits: 17
```



```
▽ TP-Originating-Address
    Length: 2 address digits
    1... .... :  No extension
    .001 .... :  Type of number: (1) International
    .... 0001 :  Numbering plan: (1) ISDN/telephone (E.164/E.163)
    TP-OA Digits: 12345000001
```

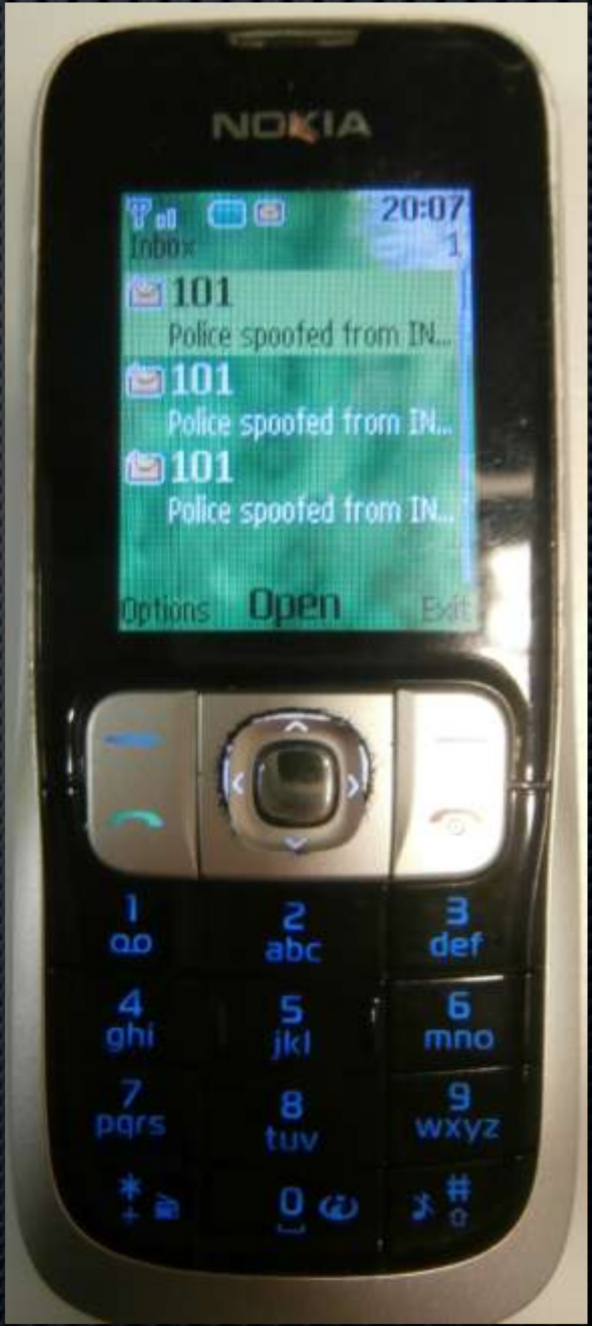


```
▽ TP-Originating-Address
    Length: 6 address digits
    1... .... :  No extension
    .101 .... :  Type of number: (5) Alphanumeric (coded according to 3GPP TS 23.038 GSM 7-bit default alphabet)
    .... 0000 :  Numbering plan: (0) Unknown
    TP-OA Digits: Hackito
```

SMS spoofing

Spoofing police !

CALL YOUR LOCAL POLICE
101
IN AN EMERGENCY ALWAYS CALL 999



101
Police spoofed from IN...

101
Police spoofed from IN...

101
Police spoofed from IN...

Also works with other special numbers:

- Emergency number
- Voice Mail number
- Operators services
- Other subscribers

Counter measures

Protecting against SMS attacks

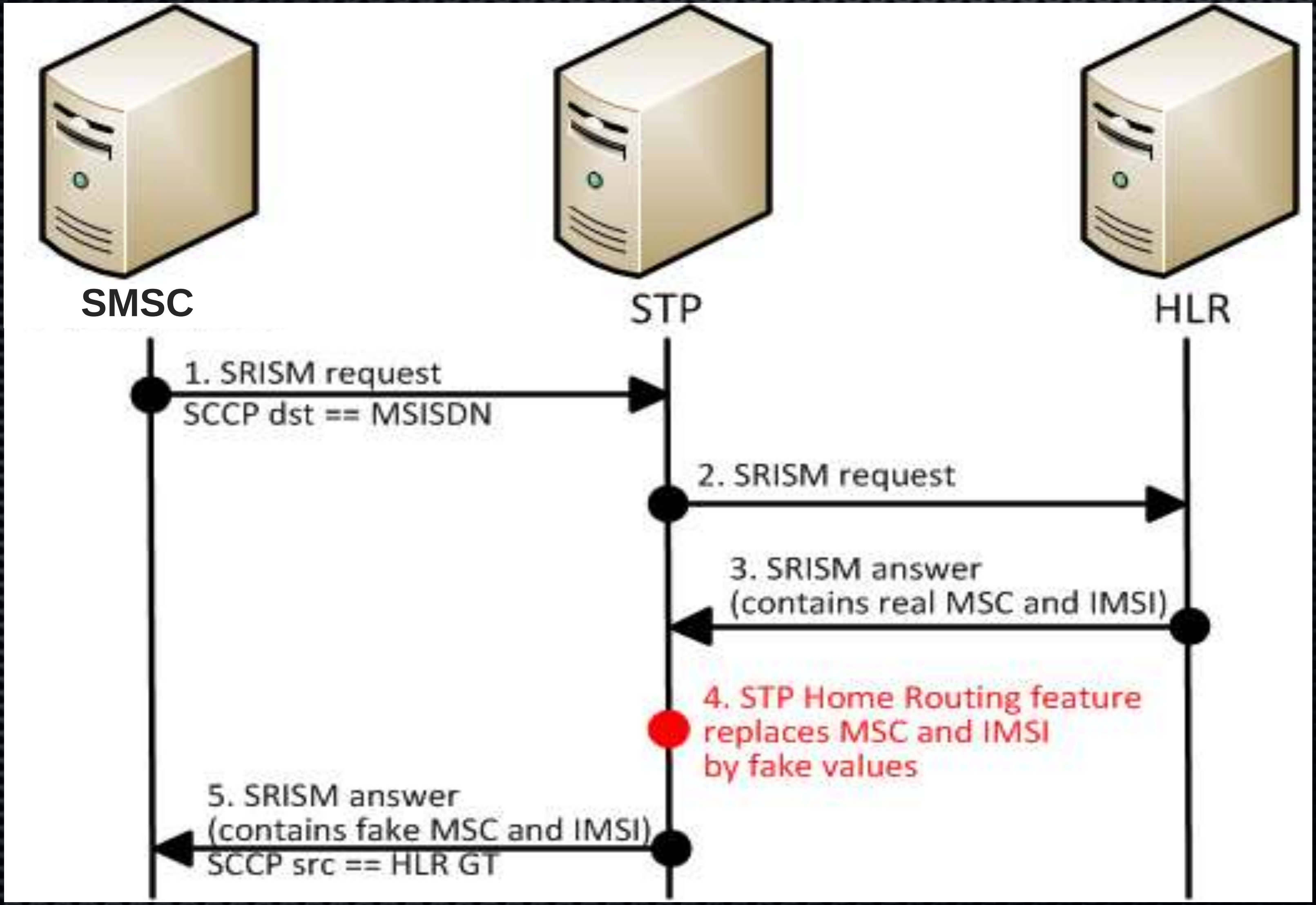
- SMS home routing
- SMS firewalls

- All incoming MAP MT Forward SM are routed to SMS firewall for inspection
- Prevents against SMS attacks:
  - SMS spam is detected and rejected
  - SMS spoofed is detected and rejected

P1 Security
Priority One Security

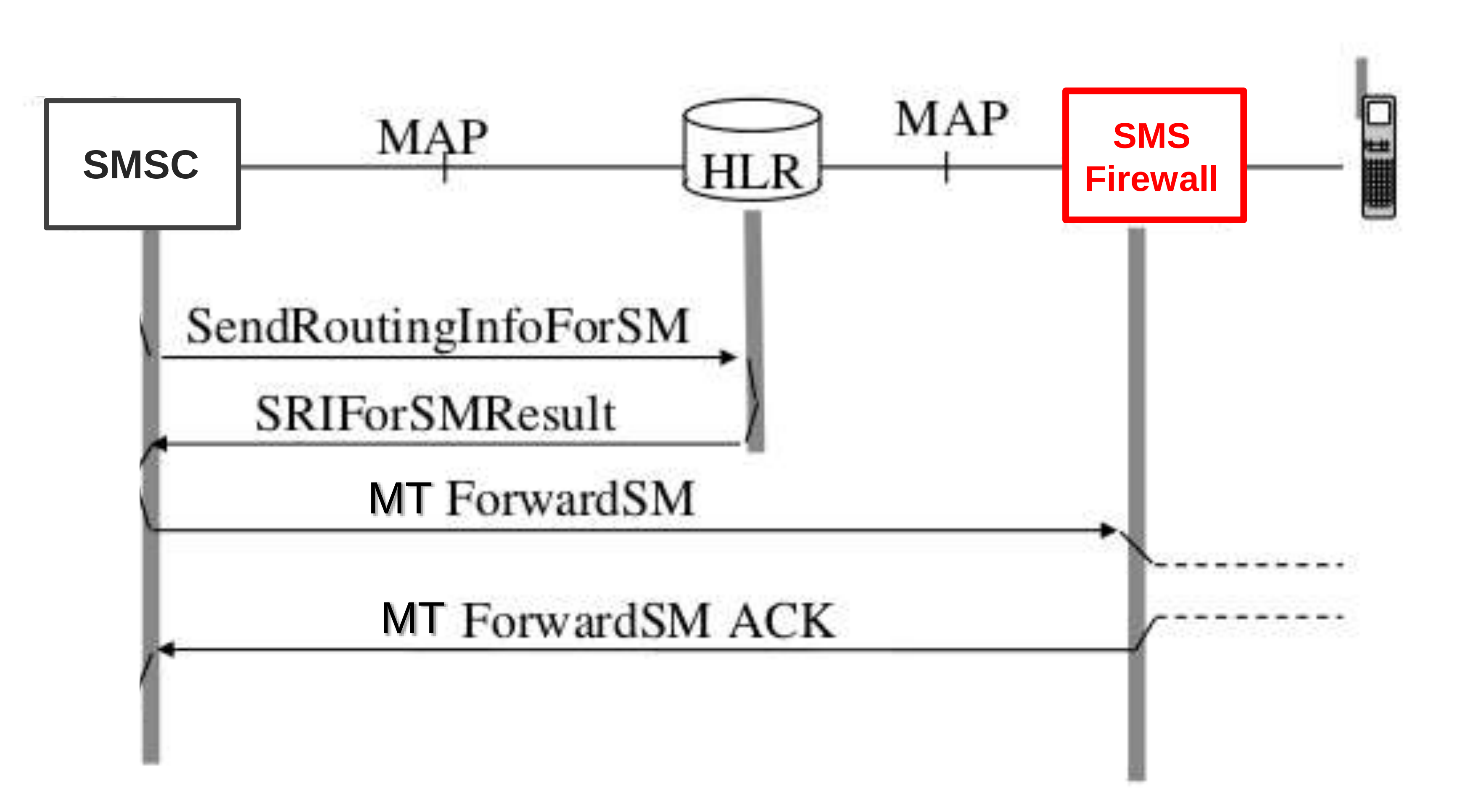
SMS Home Routing

Protecting users privacy / Protecting against spam SMS



SMS Home Routing

SMS are routed to SMS firewall for inspection



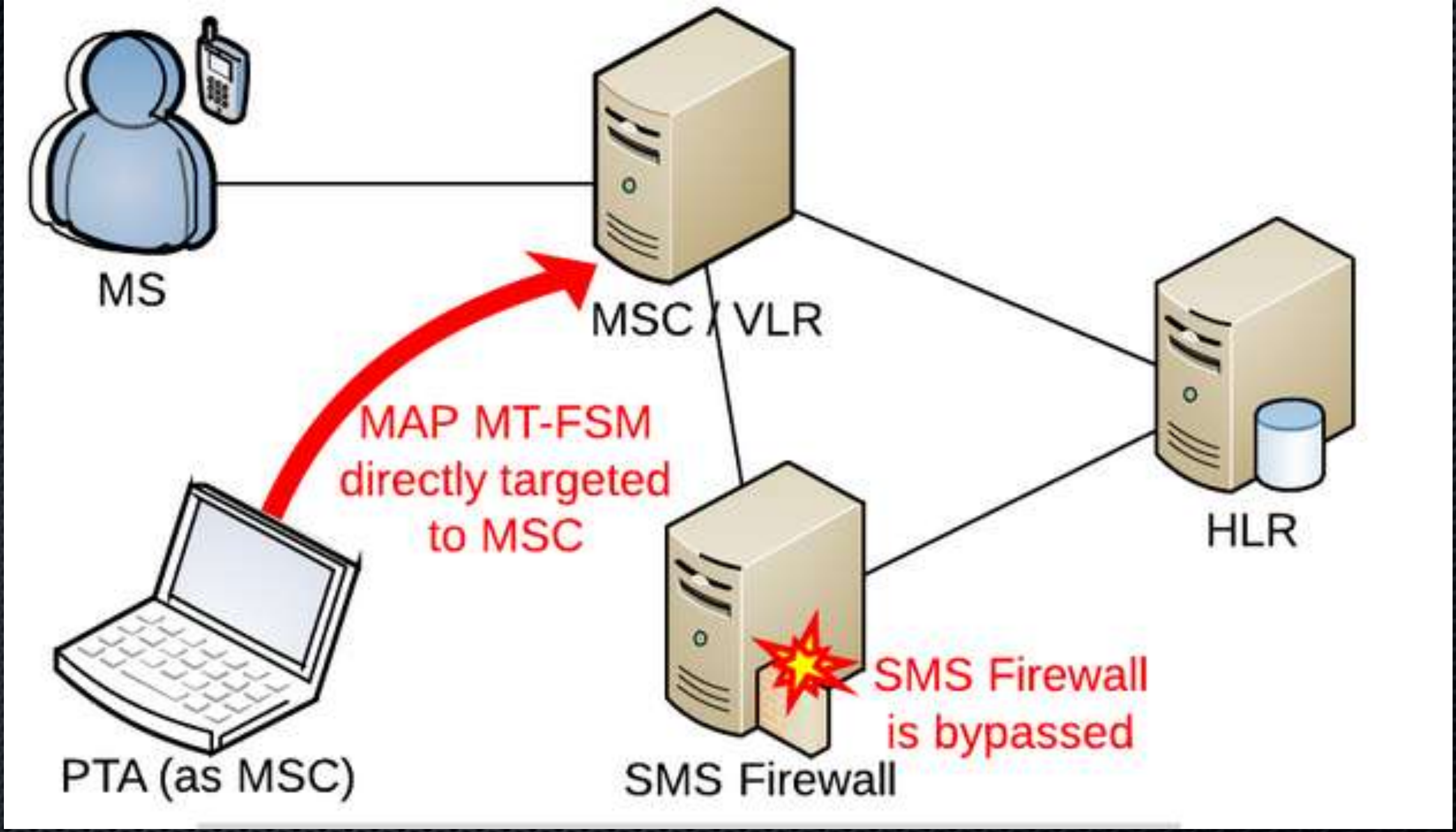
Counter Counter measures ?

How to bypass protections

- Can you actually bypass SMS firewalls ?
  - YES !
- How ?
  - Directly sending MT Forward SM to MSC
  - Route through SMS firewall is usually not enforced !
- This requires to scan and discover all available MSC prior to send SMS
  - Possible in a few hours
  - MSC number: typically < 50
- Also require target IMSI (SRI / SRISM / sendIMSI)

SMS Firewall bypassed

P1 Vulnerability Knowledge Base P1VID#112



https://saas.p1sec.com/vulns/112

Telcomap project

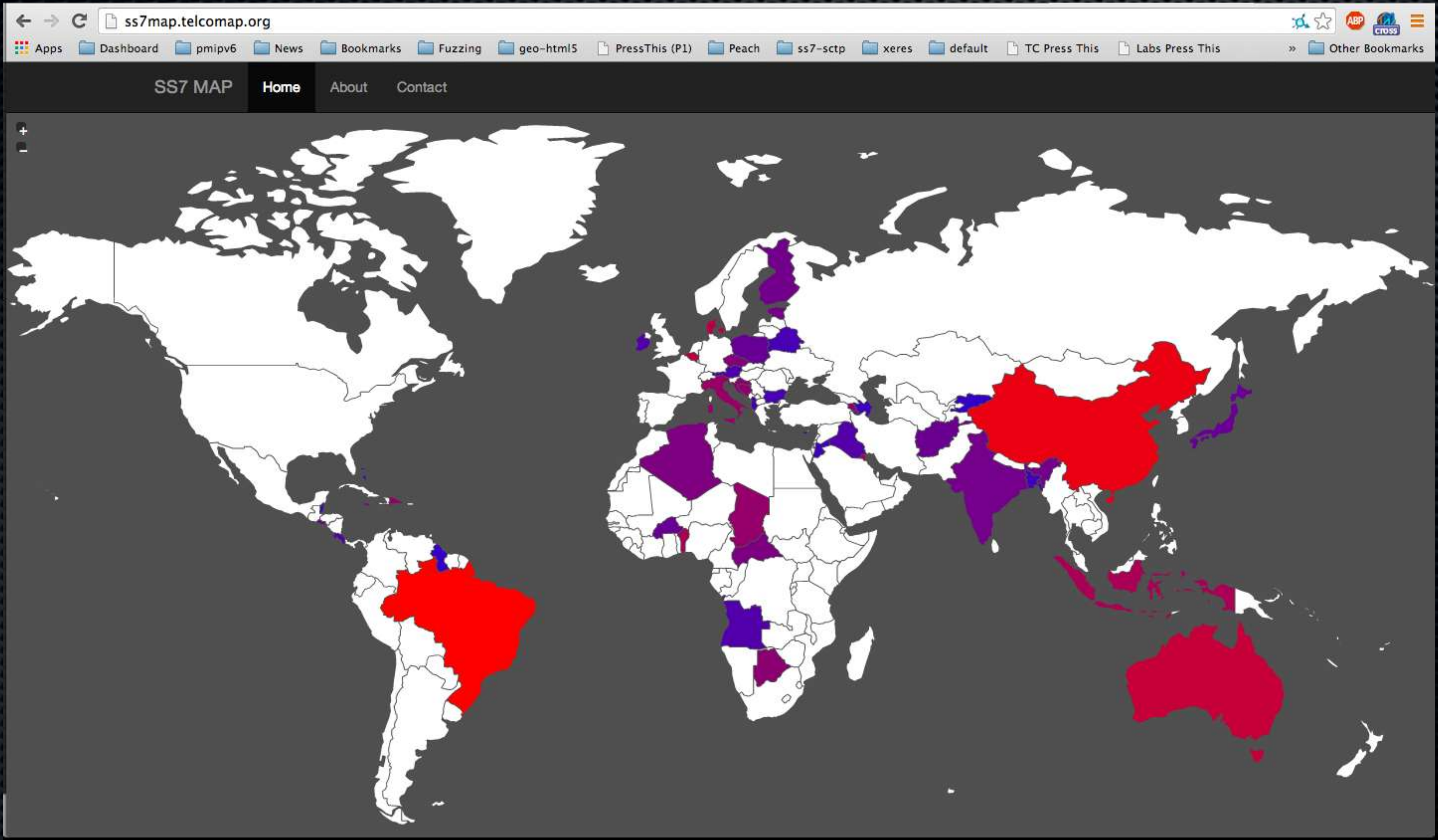
Worldwide discovery

SS7map: Scanning the worldwide SS7 network

- Discovery scan from international SS7 interconnection
- Targets: all operators / all countries
- Currently implemented testcases:
  - GT/SSN discovery scan (SCCP / TCAP)
  - MSISDN range scan (MAP SRI)
  - More to come…

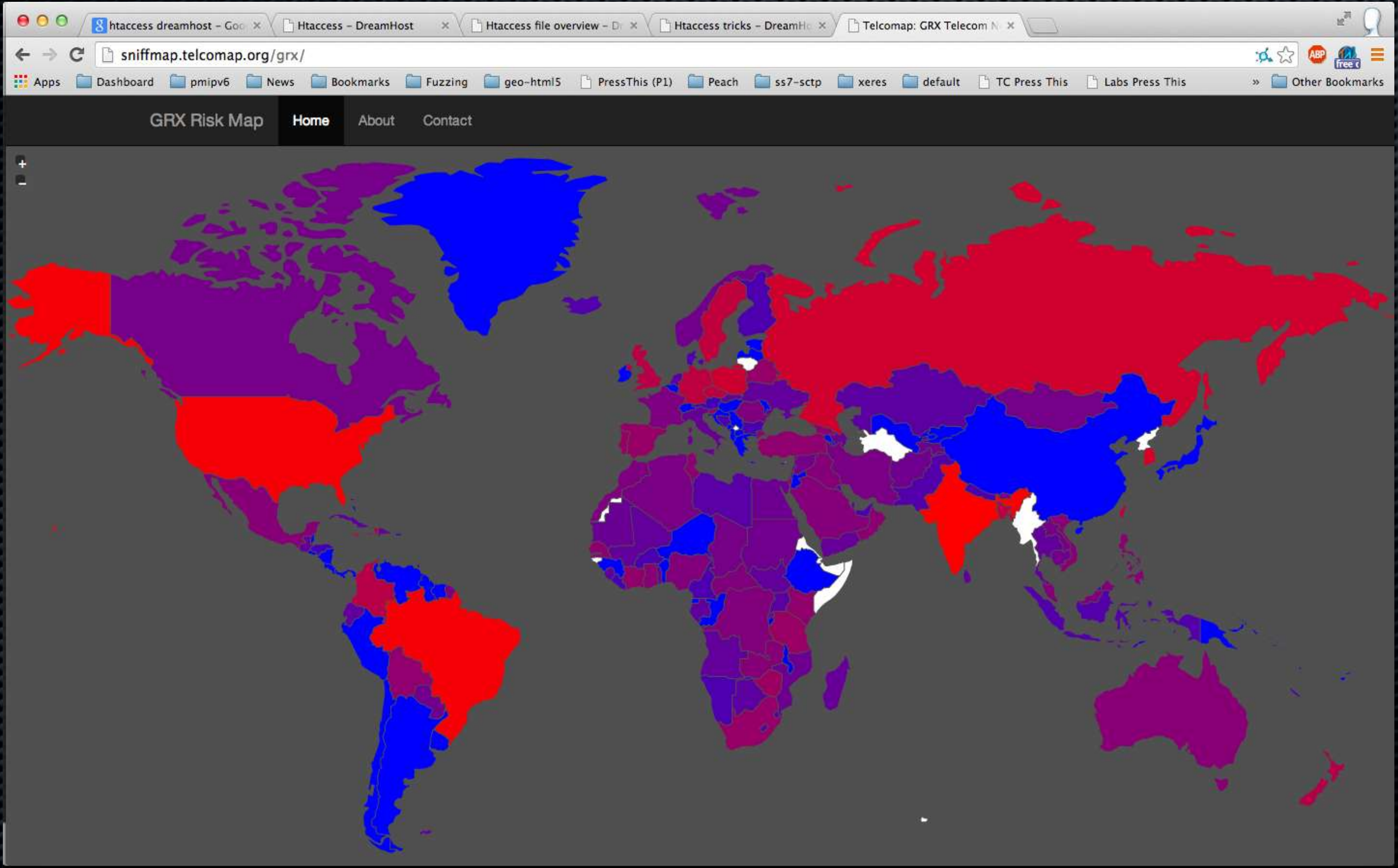
SS7 Map

Telecom Networks SS7 Exposure



GRX Map

PS, GPRS, LTE



http://sniffmap.telcomap.org/grx/

Galaxy Map

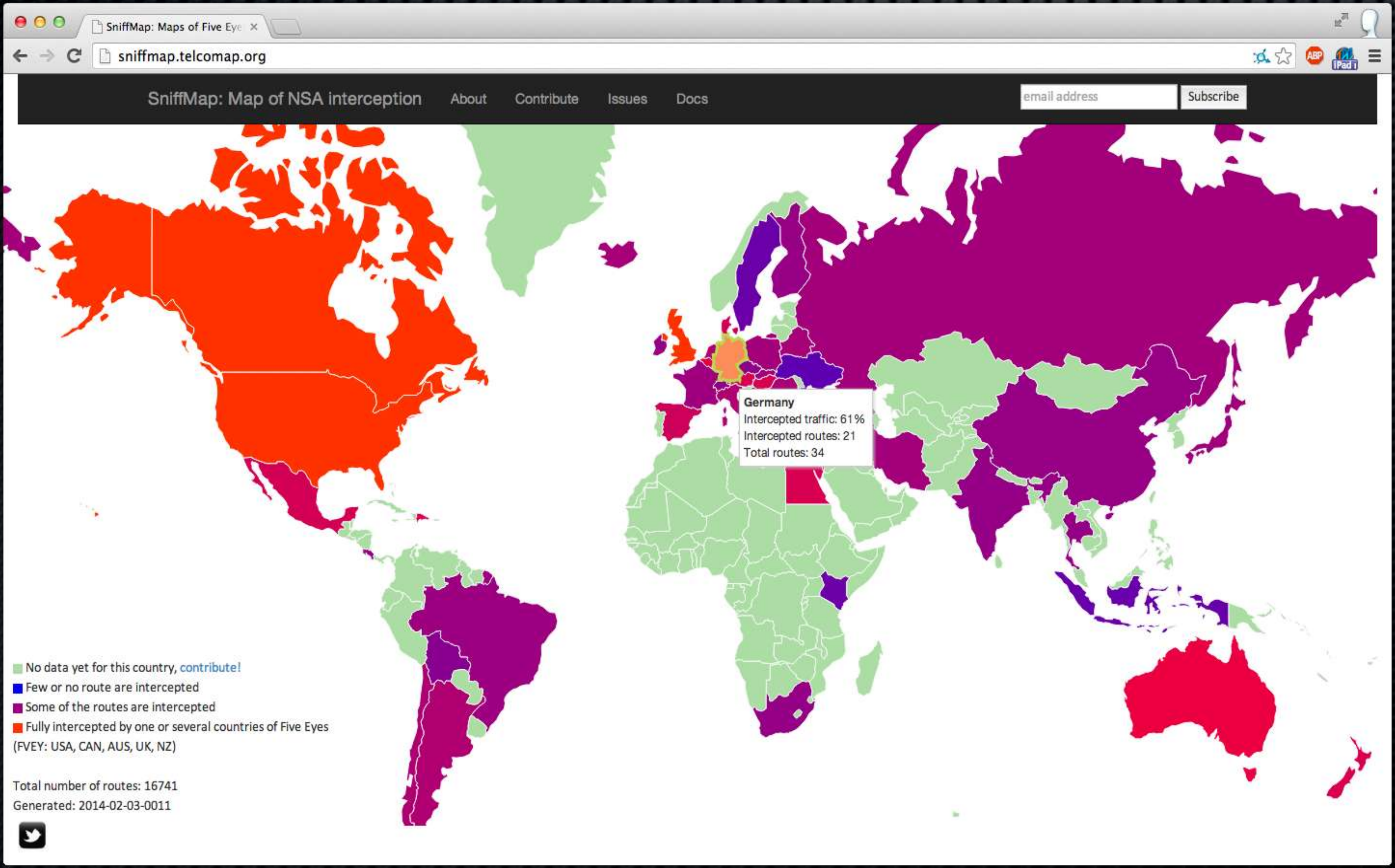
ShodanHQ-like but for Telco

Shodan is only 10% coverage of Telco OAM and Signaling

But useful to “prove” the seriousness: anyone can get access…
from Internet

Sniffmap

Map of Five Eyes interception



Germany
Intercepted traffic: 61%
Intercepted routes: 21
Total routes: 34

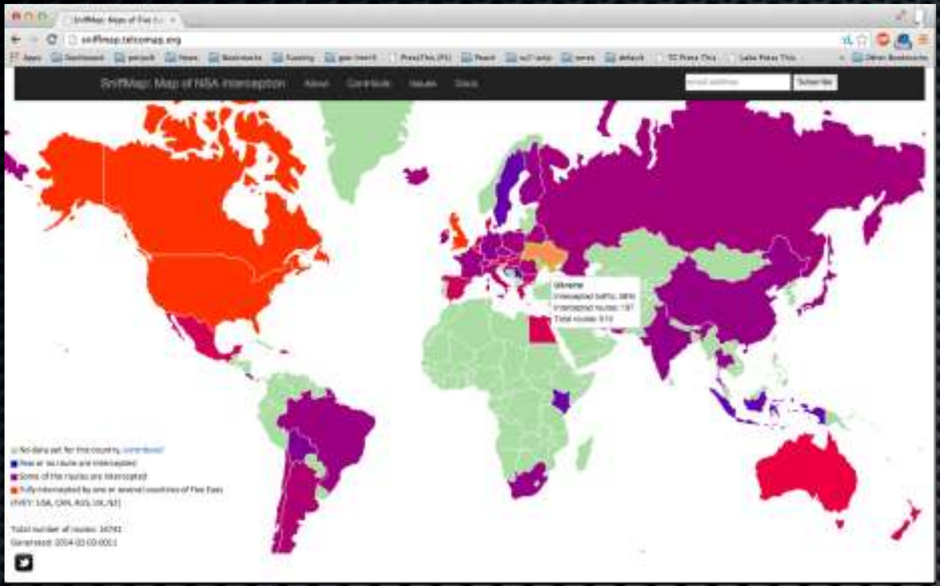
🟩 No data yet for this country, contribute!
🟦 Few or no route are intercepted
🟪 Some of the routes are intercepted
🟧 Fully intercepted by one or several countries of Five Eyes
(FVEY: USA, CAN, AUS, UK, NZ)

Total number of routes: 16741
Generated: 2014-02-03-0011

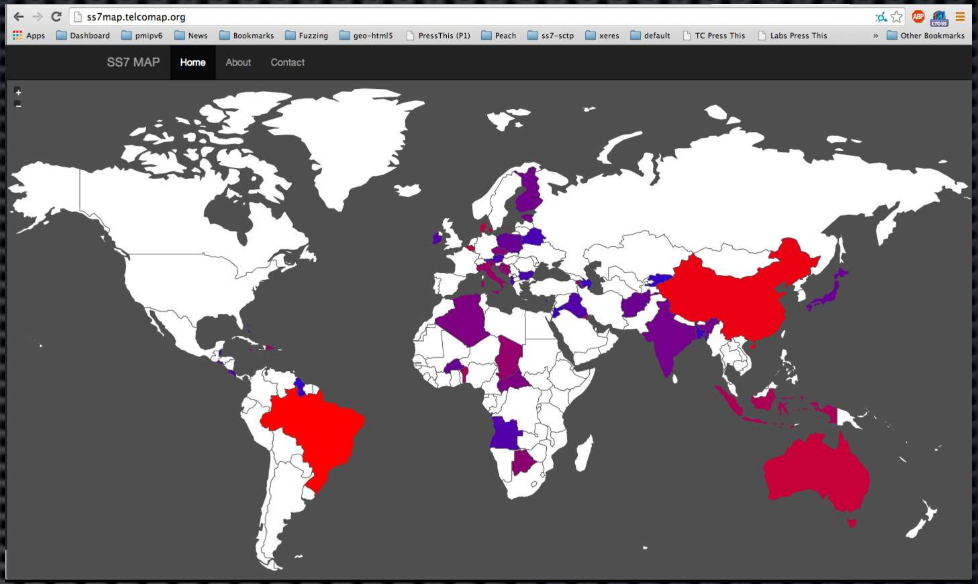
http://sniffmap.telcomap.org/

Attack surface

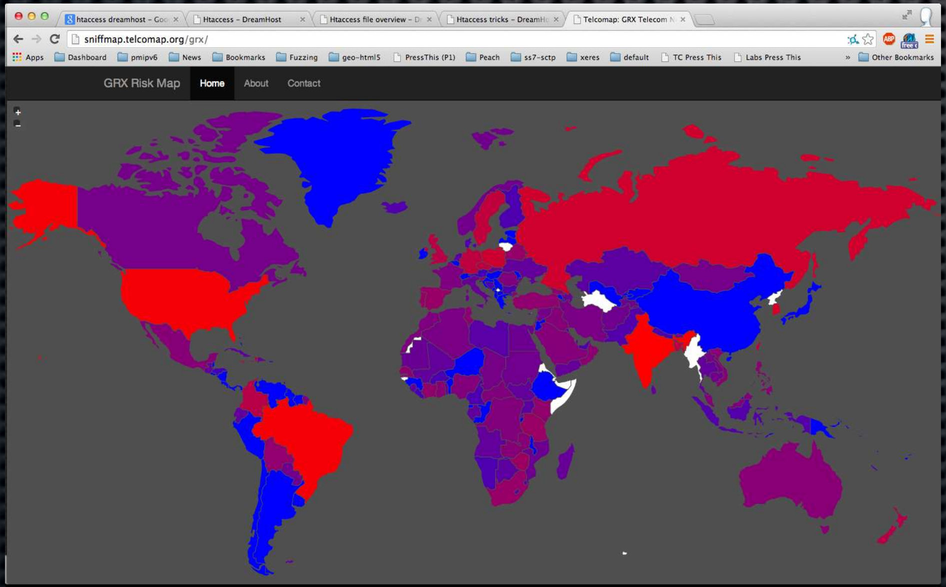
Telcomaps


sniffmap.telcomap.org
SniffMap: Map of NSA interception
About
Contribute
Issues
Docs
Subscribe
Ukraine
Intercepted traffic: 38%
Intercepted routes: 197
Total routes: 510
No data yet for this country, contribute!
Few or no route are intercepted
Some of the routes are intercepted
Fully intercepted by one or several countries of Five Eyes
(FVEY: USA, CAN, AUS, UK, NZ)
Total number of routes: 16793
Generated: 2014-03-03 0011

Sniff Map



SS7 Map



GRX Map

Galaxy Map

Going further

- MAP specification: 3GPP TS 29.002
  http://www.3gpp.org/DynaReport/29002.htm
- SMS specification: 3GPP TS 23.040
  http://www.3gpp.org/DynaReport/23040.htm
- SMS Home routing specification: 3GPP TS 23.840
  http://www.3gpp.org/DynaReport/23840.htm
- Locating mobile phones using MSC GT (CCC)
  http://events.ccc.de/congress/2008/Fahrplan/attachments/1262_25c3-locating-mobile-phones.pdf
- Description of MAP usual callflows
  http://www.netlab.tkk.fi/opetus/s383115/2007/kalvot/3115L7-9e.pdf
- P1 Security SaaS and Vulnerability Knowledge Base
  https://saas.p1sec.com/
- SMS Gateways
  http://www.vianett.com/
- Open Cell ID databases / API
  http://opencellids.org/

Thank you !
Questions ?

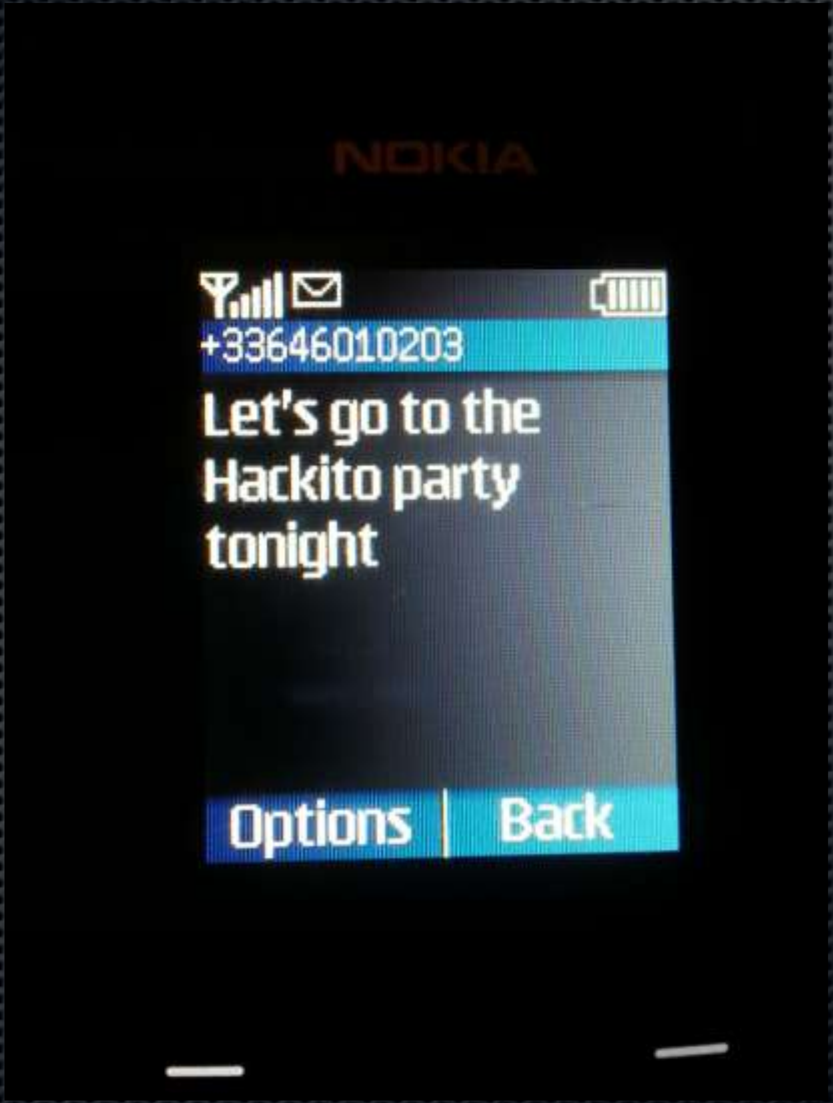
P1 Security
Priority One Security

http://www.p1sec.com

Thanks to
P1 Security team

Questions to:
po@p1sec.com
alex@p1sec.com

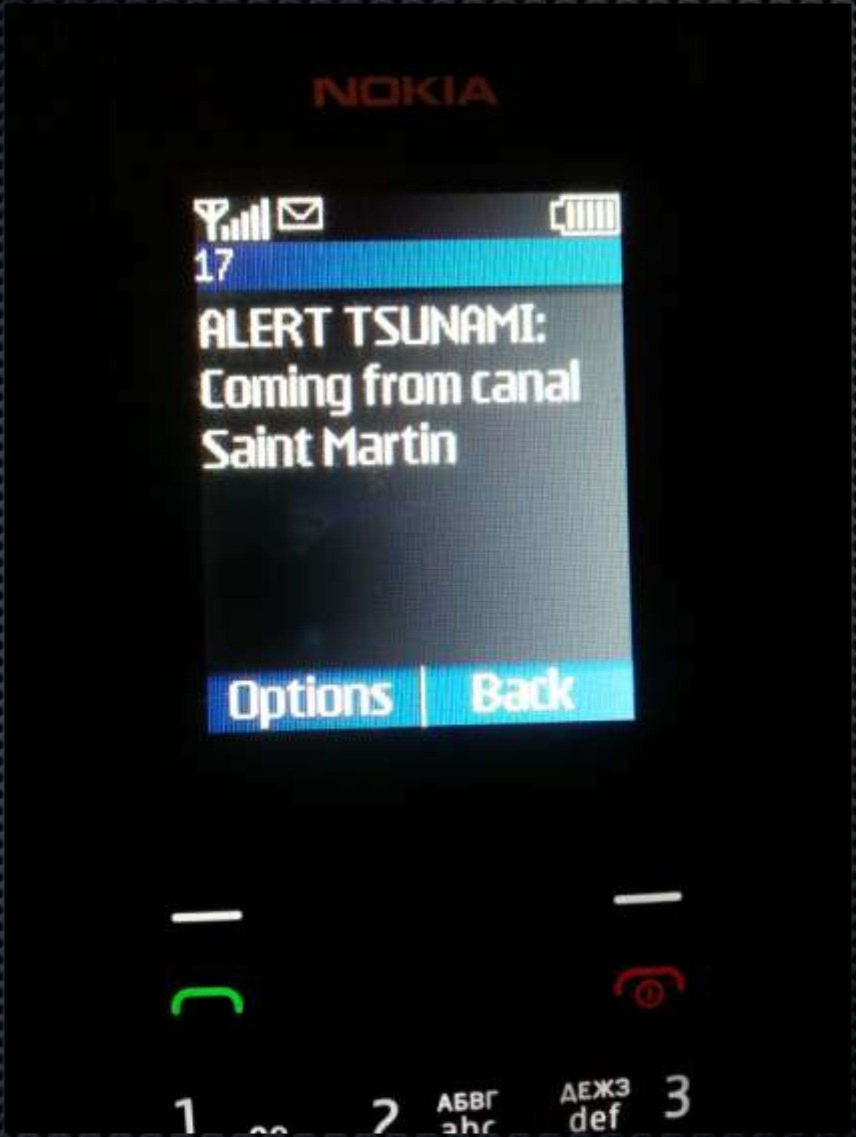
Back up demo



+33646010203

Let's go to the Hackito party tonight

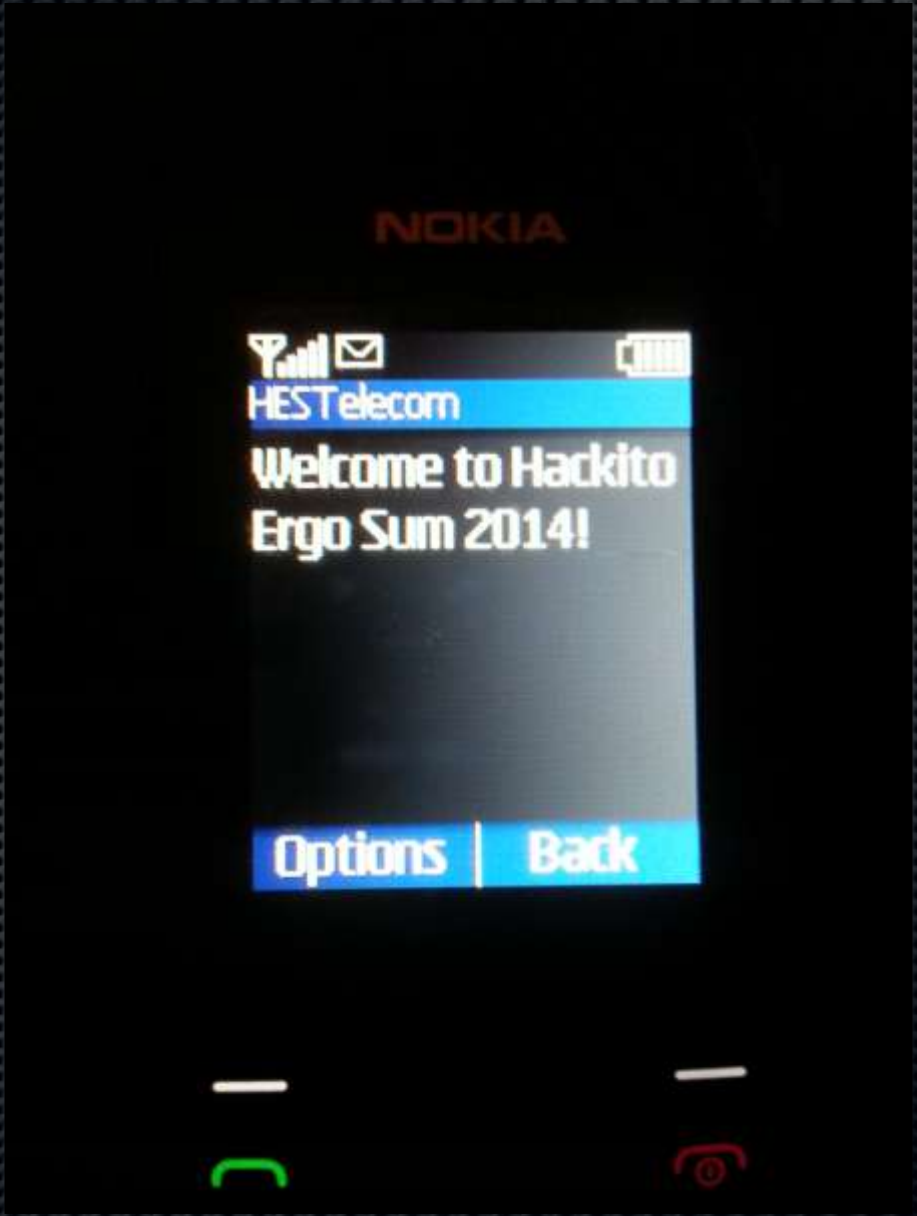
Back up demo



17

ALERT TSUNAMI: Coming from canal Saint Martin

Back up demo



HESTelecom

Welcome to Hackito Ergo Sum 2014!