1. **Parametros iniciales**

SourcePort: 40150
DestinationPort: 4729
Dst/SrcIP: lo

Procedimiento General (Induciendo Mensajes):

GSMTAP 87 (CCCH) (RR) Paging Request Type 1
GSMTAP 87 (CCCH) (RR) Immediate Assignment
LAPDm 81 U P, func=SABM(DTAP) (RR) Paging Response
GSM SMS 87 I, N(R)=0, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)

Procedimiento General (Cuando se conecta por primera vez):

GSMTAP 87 (CCCH) (RR) Immediate Assignment (Downlink)
I, N(R)=1, N(S)=0(DTAP) (MM) Identity Response (UPLINK)
I, N(R)=2, N(S)=3(DTAP) (MM) Location Updating Accept (Downlink)

Se debe tener claridad si corresponde TA **Immediate Assignment** del abonado.

2. **Obtener el mensaje sent**

Estos tipos de mensaje vienen fragmentados, por lo cual necesita ensamblar los mensajes. El primer mensaje es fragmentado, su mensaje consecuente es RP-DATA. Luego de obtener ambos mensajes, se concede a ensamblar.

Para lo anterior es supremamente importante identificar el mensaje fragmentado y el mensaje RP-DATA. De igual manera, el algoritmo debe ser suficiente para descartar los demás mensajes tipo LAPDm. Pues ambos mensajes tiene un su empaquetado al menos un capa de protocolo LAPDm.

El algoritmo antes de ensamblar debe saber POR LO MENOS LA LONGITUD DE PAYLOAD DE AMBOS MENSAJES. Igualmente como atributos del mensaje ensamblado es necesario guardar:

Tipo de Canal
ARFCN
ISDN Origen
Contenido del mensaje

Offset FrameNumber between these message is: 51

Dos mensajes, es el número máximo que se pueden ensamblar siempre en cuando un ISDN+mensaje no supere más de 14 items. Pues existirá más de un mensaje FRAG, y solo está diseñado para sincronizar un solo segmento. El ISDN no puede superar más de 4 items.

> *La idea es sumar lo que siempre va más la longitud del ISDN (Tener en cuenta que un par de ISDN es una posición) desde el resultado empieza el char donde indica la posición del la longitud del mensaje. Como está diseñado para dos char entonces max y minimo son 4 y 3 números.*

LAPDm 87 I, N(R)=0, N(S)=0 (Fragment)

```
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
0000  00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010  00 49 3a 16 40 00 40 11 02 8c 7f 00 00 01 7f 00
0020  00 01 9c d6 12 79 00 35 fe 48 02 04 01 00 83 2a      0x832a & 0x3fff ARFCN
0030  00 00 00 07 71 37 07 00 00 00 0f 00 53 69 01 21      00077137 = 487735 (FrameNumber)
                                                          07  Canal SDCCH/ 3 --1-(More Sg)
0040  01 d6 03 a1 00 00 00 19 04 03 a1 11 f1 00 00 91
0050  30 8b f5 ab 5f bb 00
```

0x3C 53 01010011

```
010100 . .   longitud 20   hex(0x3c + (0x53>>2))
. . . . . 1 .   MoreSegment
. . . . . . . 1   final Octet   hex(0x3c & 0x03)  debe ser igual a 3
```

GSM SMS 87 I, N(R)=0, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)

```
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
0000  00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010  00 49 3a 57 40 00 40 11 02 4b 7f 00 00 01 7f 00
0020  00 01 9c d6 12 79 00 35 fe 48 02 04 01 00 83 2a      0x832a & 0x3fff ARFCN
0030  00 00 00 07 71 6a 07 00 00 00 0f 02 41 60 32 90      0007716a = 487786 (Frame Number)
                                                          07  Canal SDCCH/4 3 ---0-(more S)
0040  50 0a 0b 70 79 bd 2c 0e 93 d7 f2 18 08 2b 2b 2b
0050  2b 38 bf b1 2c cc 00
```

0x3C 41 01000001

```
010000 . .   longitud 16   hex(0x3c + (0x41>>2))
. . . . . 0 .   MoreSegment
. . . . . . . 1   final Octet   hex(0x3c & 0x01)  debe ser igual a 1
```

Message Reesambly

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000	69	01	21	01	d6	03	a1	00	00	00	19	04	03	a1	11	f1
0010	00	00	91	30	60	32	90	50	0a	0b	70	79	bd	2c	0e	93
0020	d7	f2	18	08												

03 a1 11 f1 **0x0C** longitud=3

11 f1 → Numero origen seria : **0E**(0)+**0E**(1)+**0F**(0)

0b **0x19** longitud del mensaje desde 0x19 - 0x23 = 0x19 + (0x0b-1)

>>> hex(0x19+0x0b-1)
'0x23'

https://en.wikipedia.org/wiki/GSM_03.38#GSM_7-bit_default_alphabet_and_extension_table_of_3GPP_TS_23.038_.2F_GSM_03.38
Converter from from 1A-22
http://smstools3.kekekasvi.com/topic.php?id=288
http://www.rednaxela.net/pdu.php

3. Paging Procedures !

Evidentemente existen dos tipos Paging con diferente canal Lógico. CCCH para Request y SDCCH/4 para Response. Request siempre es un canal tipo Downlink y Response de Downlink/Uplink. Preliminarmente nos interesamos por el segmento Paging Response con canal de Subida **U,Pfunc=SABM(DTAP) (RR) Paging Response**.

Paging Response es un segmento que siempre aparece cuando recibe un mensaje SMS **GSM SMS 87 I, N(R)=0, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-DATA** al MS. Notificando primero por parte de OpenBTS un Paging Response **U F, func=UA(DTAP) (RR) Paging Response** de canal Downlink, y luego por parte de MS responde con un Paging Response **U,P func=SABM(DTAP) (RR) Paging Response**.

Pero, Si se envían de manera consecutiva menor a medio segundo, OpenBTS no registra un paging Response sino hasta después de un tiempo moderado (Mejor a más de un minuto) del **GSM SMS 87 I, N(R)=0, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-DATA** enviado. Primero se registra el doble camino de Paging Response y después el procedimiento de ensamblaje del SMS (Mensaje RP y Fragmentos consecuentes).

Paging Response siempre va a contener una identidad (TMSI/IMSI). En cambio un paging Request no siempre contiene identidad, es decir, dicho campo de la trama (TMSI/IMSI) se envía de forma NULA (2b). OpenBTS registra de manera unilateral (De un solo camino) varios Paging Request de manera reiterada correspondiente a la configuración de la combinación de

canales lógicos de OpenBTS. Prematuramente al análisis efectuado los Paging request no corresponden a los eventos de los sms **GSM SMS 87 I, N(R)=0, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-DATA** como si lo hacen los paging Response. Ṕor ello es importante descartar los paging Requests cuyo (TMSI/IMSI) están vacios o nulos.

Pero si existe correlación con los números de tramas paging del mismo tipo de canal. Es decir a partir del primer paging efectivo (Contiene TMSI/IMSI) se puede conocer a partir de su número de trama cuando va dar lugar el siguiente paging efectivo. Para Response la constante es 36 y Request es 51. Esta correlación nos puede ayudar para determinar cuándo se va a registrar el siguiente paging Request efectivo. Pues Paging Response siempre contiene un IMSI/TMSI y se registra cada cuando existe un evento de tipo **GSM SMS 87 I, N(R)=0, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-DATA**. (*Cada ciclo es un par Paging Request. Entre cada trama que conforma el ciclo hay un offset de 51 Frames . Y por cada ciclo hay un offset de 3366 Frames. Un inicio de cada ciclo se toma por la primera trama de cada Par.*)**(No es una constante que siempre sucede)

CCCH Channel

(CCCH) (RR) Paging Request Type 1 (DOWNLINK)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000	00	00	00	00	00	00	00	00	00	00	00	00	08	00	45	00
0010	00	49	47	5e	40	00	40	11	f5	43	7f	00	00	01	7f	00
0020	00	01	9c	d6	12	79	00	35	fe	48	02	04	01	00	83	2a
0030	00	00	00	07	7d	25	02	00	00	00	25	06	21	10	05	f4
0040	00	06	88	2f	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b
0050	2b	5d	eb	c3	16	eb	00									

21 **Tipo de mensaje:** Paging Request Type 1
02 **Tipo de Canal :** CCCH

TMSI (8 Numbers)--> 00 06 88 2f 0x0006882f
Longitud Tmsi: 05
Identificador TMSI: f4
. . . . . 100 Tipo TMSI
1111. . . . do not matters
. . . . 1. . . even (Par)

SDCCH/4 Channel

U,Pfunc=SABM(DTAP) (RR) Paging Response (UPLINK)

```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
0000   00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010   00 43 47 FF 40 00 40 11 f4 a8 7f 00 00 01 7f 00
0020   00 01 9c d6 12 79 00 2f fe 42 02 04 01 00 c3 2a   c3 Uplink
0030   00 00 00 07 7d a0 07 00 00 00 01 3f 35 06 27 00   07 SDCCH4 27 P.REsponse
0040   03 30 58 a2 05 f4 00 06 88 2f 2b 2b 2b 2b 2b 2b
0050   2b
```

c3 Uplink

. 1 . . . . . Uplink
. 0 . . . . . Downlink

IMSI (8 Numbers)--> 23 01 51 41 68 16 01 732101514866110
Longitud IMSI: 08
Identificador TMSI: 79
. . . . . 001 Tipo IMSI
0111. . . . do not matters
. . . . 1. . . odd (impar)

TMSI (8 Numbers)--> 00 06 88 2f 0x0006882f
Longitud Tmsi: 05
Identificador TMSI: f4
. . . . . 100 Tipo TMSI
1111. . . . do not matters
. . . . 1. . . even (Par)

I, N(R)=1, N(S)=0(DTAP) (MM) Identity Response (UPLINK) --IMSI

```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
0000   00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010   00 43 40 55 40 00 40 11 fc 52 7f 00 00 01 7f 00
0020   00 01 9b bd 12 79 00 2f fe 42 02 04 01 00 40 b1
0030   00 00 00 1e 92 74 07 00 00 00 01 20 2d 05 59 08
0040   79 23 01 51 41 68 16 01 2b 2b 2b 2b 2b 2b 2b 2b
0050   2b
```

07 Tlpo de Canal: SDCCH/4
40 **Uplink**
. 1 . . . . . Uplink

. 0 . . . . . Downlink

59Tipo de Mensaje : **Identity Response**
. . 01 1001 **Identity Response == 0x19**

IMSI (14 Numbers)-->79 **23 01 51 41 68 16 01** 732101514866110
Longitud IMSI: 08
Identificador IMSI: 79
. . . . . 001 Tipo IMSI
0111. . . . do not matters
. . . . 1. . . odd (impar)

IMEI(8 Numbers)--> **23 01 51 41 68 16 01** 732101514866110
Longitud IMEI: 08
Identificador IMEI: 8a
. . . . . 010 Tipo IMEI
1000. . . . do not matters
. . . . 1. . . odd (impar)

U F, func=UA(DTAP) (RR) Paging Response (DOWNLINK)

4. **Timing Advance Procedures**

LAPDm 87 U, func=UI(CCCH) (RR) System Information Type 6
LAPDm 81 U, func=UI(DTAP) (RR) Measurement Report
LAPDm87 U, func=UI(CCCH) (RR) System Information Type 5

GSMTAP 87 (CCCH) (RR) Immediate Assignment

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000	00	00	00	00	00	00	00	00	00	00	00	00	08	00	45	00
0010	00	49	39	6c	40	00	40	11	03	36	7f	00	00	01	7f	00
0020	00	01	9c	d6	12	79	00	35	fe	48	02	04	01	00	83	2a
0030	00	00	00	07	70	98	02	00	00	00	2d	06	3f	00	20	03
0040	2a	18	7b	07	00	00	2b	2b	2b	2b	2b	2b	2b	2b	2b	2b
0050	2b	5d	eb	c3	16	eb	00									

02 Tipo de Canal: CCCH
3f Tipo de mensaje: Immediate Assignment
00 Valor de Timing Advance: 0 (0x44)

5. **Protocols Stacks (BCCH Do not matters)**

CCCH:

GSMTAP 87 (CCCH) (RR) Immediate Assignment

GSMTAP 87 (CCCH) (RR) Paging Request Type 1

SDCCH/4:

LAPDm 81 U P, func=SABM(DTAP) (RR) Paging Response

LAPDm 87 U F, func=UA(DTAP) (RR) Paging Response

GSM SMS 87 I, N(R)=0, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-DATA (Network to MS)

LAPDm 81 I, N(R)=2, N(S)=0(DTAP) (SMS) CP-ACK

LAPDm 81 I, N(R)=2, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-ACK (MS to Network)

I, N(R)=1, N(S)=0(DTAP) (MM) Identity Response

SACCH/4:

LAPDm 87 U, func=UI(CCCH) (RR) System Information Type 6

LAPDm 81 U, func=UI(DTAP) (RR) Measurement Report

LAPDm87 U, func=UI(CCCH) (RR) System Information Type 5