CyberHack Magazine #3

ESPECIAL MÓVILES (1ª Parte)

Indice:

0.- INTRODUCCIÓN.

Hace ya bastante tiempo desde que salió el número dos, pero sin colaboración es casi imposible sacar a la luz una buena revista. Así que para aquellos que les guste mucho leer y gorronear al máximo... seguid así que sin investigar no llegareis a nada. A partir de ahora a parte de en IBERHACK, las revistas tienen su propia página WEB:
HTTP://WWW.GEOCITIES.COM/SILICONVALLEY/PINES/2558/
y dirección de correo electrónico para las correspondientes colaboraciones a cyberhackcy@geocities.comallí encontrareis las últimas versiones de la revista y aclaraciones correspondientes... pero por favor, el correo electrónico es gratis y no cuesta nada una simple opinión o una jodida colaboración. De todos modos un saludo a saqueadores, webhack y a todos los demás.

Debido a lo largo que se hace la recopilación de información de estos temas hemos decidido realizarla en dos partes. En esta primera solo será acerca de losmoviles... Y en la segunda, trataremos explosivos y otras cosas de mayorinteres para otros.

1.- MOTOROLA GSM.

Bueno, vamos a estudiar un poco la parte técnica de los teléfonos móviles y en general de motorola, pero antes una pequeña introducción al sistema GSM.

La diversidad de sistemas de telefonía en el mundo ha forzado a tomar un estandar en la llamada red de telefonía mundial, así se podría utilizar el mismo teléfono en distintos países del mundo pretendiendo reservar dos rangos de frecuencias en la banda de los 900 Mhz. Las redes

actuales emplean ofertas tales como transmisión de datos, voz, teleservicios, identificación del número llamante (muy util para cuando pinchas una línea saber que numero es, eso sí, si es digital), SMS (shot message system), fax, etc. Esto convierte al terminal no en un simple teléfono sino en una oficina de bolsillo, estando localizado en gran parte del mundo. Las características principales del sistema GSM son:

· Un sistema uniforme para todos los países.
· El sistema debe permitir el uso de sistemas de bolsillo.
· Debe soportar varios usuarios por red.
· Alta calidad de sonido y ancho de banda.
· Alto sistema de seguridad.
· Banda de frecuencias de 850-915 MHz. y de 935-960 MHz.

Gracias al sistema GSM totalmente digital, cada canal puede ser dividido en ocho subdivisiones de tiempo, con una longitud de 0.577 mx. Cada una, y la banda de frecuencias está dividida en 124 canales, cada uno con un ancho de banda de 200 Khz. Estos canales son cortados en ocho tramos, creando una combinación de multiplexación de frecuencia y tiempo (TDMA/FDMA). Este sistema permite establecer ocho llamadas en un mismo canal de manera simultanea, así solo se necesita un modulo transmisor/receptor en el repetidor.

Una vez visto el funcionamiento de un sistema GSM por encima, vamos a tratar el caso en nuestro país con nuestras queridas compañías, Timofónica y Airrapel (Adivina cuando se te van a cortar las llamadas).

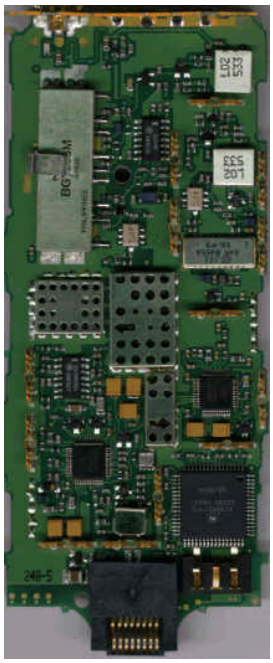
· SIM-LOCKING: Aunque en algunos países está prohibido, en nuestro país es una realidad, los operadores bloquean los teléfonos, para que solo puedan ser utilizados con sus tarjetas, y cuando pasa un periodo de tiempo como un año, que se supone que ya has abonado el teléfono, llamas y a partir del IMEI (numero de serie), te dan un código de desbloqueo a partir de este, por eso es distinto para cada teléfono. Hasta ahora estamos investigando sobre el tema, pero si alguien sabe cual es la ansiada fórmula por favor que mande un E-Mail.

MOTOROLA 7500:

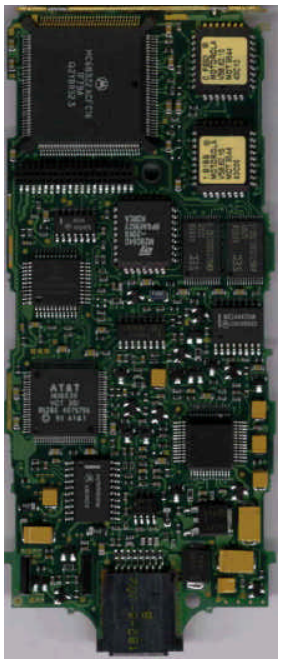
Aunque parece de juguete por su tapadera (flip phone) y su antena como el palo de un chupa-chups, es un gran teléfono con las mismas funciones que el motorola 6200 flare.

La distribución de sus componentes internamente queda tal que así:

Lector de tarjeta



Cara emisor

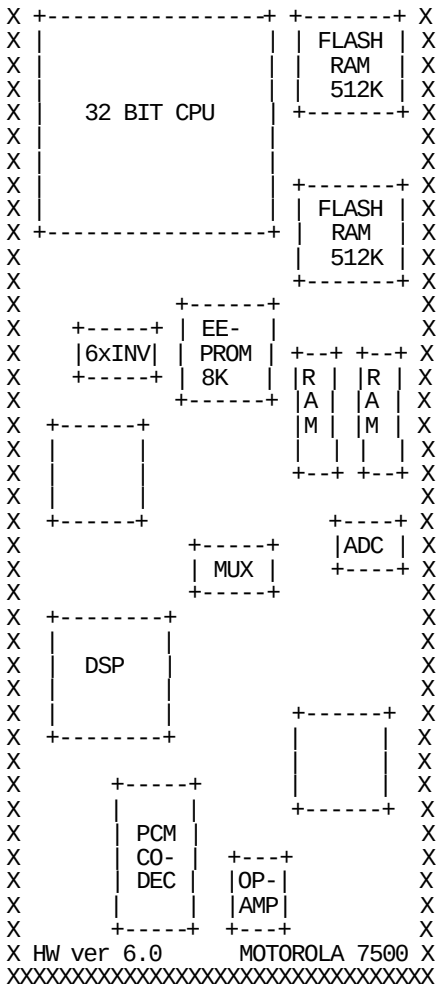


Cara componentes

Aunque la que más nos interesa es la cara de los componentes:

```
MOTOROLA MICRO TAC INTERNATIONAL 7500 GSM CHIPLIST RF-BOARD FRONT
=================================================================

 1) MC68332ACFC16     Motorola 68K family 32 bit CPU 16 MHz with 2K TPURAM

 2) 2 x AM29F040-120 AMD Flash memory 512K x 8  (4 Mbit) 120 ns

 3) 2 x KM62256 –7 SECStatic RAM 32K x 8  (256 Kbit) 70 ns

 4) M28C64C-20K6      SGS-T  EEPROM 8K x 8 (64Kbit) 200ns

 5) 74AC04 Motorola 6 x 2 State inverters

 6) 43E07, SCV38138CB05 Motorola     ???

 7) 14051B Motorola 8 Ch Analog multiplexer / demultiplexer

 8) MC14447DW Motorola8 - 10 bit, 6 ch ADC

 9) AT&T 1616S30      Lucent DSP incl. 12Kx16 bit ROM & 2Kx16 bit DPRAM

10) 99T30, SC79954FB Motorola???

11) MC145480DW Motorola      PCM CODEC Filter Mu / A- Law

12) 33172, 4YNL Motorola     Dual Operational Amplifier
```

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
X                                    X
```



El chipset del motorola 7500 versión Hardware 6.0. con una pequeña información acerca de alguno de sus componentes.

PINOUTS:

Motorola Flip Pinout:

Modelos (5200,7200,7500)

(Numerado de izquierda a derecha , teclado arriba y la bateria abajo). –

1) Gnd
2) Pos (Vcc)
3) True data (TD) (input)
4) Complimentary data (CD) (input)
5) Return data (RD) (output)
6) Audio gnd
7) Audio out
8) Audio in

No se puede conectar el micro entre los pines 1 & 8 y los altavoces entre los pines 1 & 7 para hacer un manos libres. El teléfono necesita saber cuando está existente un kit de manos libre, por eso no aparece el menú.

Modelos (6200, 8200, 8400)

(Numerado de izquierda a derecha, Teclado arriba y bateria abajo)

1) Audio Ground
2) V+
3) True data (TD) (input)
4) Complimentary data (CD) (input)
5) Return data (RD) (output)
6) GND
7) Audio Out - on/off
8) Audio In
9) Manual Test - ???
10) Battery Feedback
11) Antenna connector

Bueno, una vez estudiado el Motorola y que modelo es, pasamos a introducir el siguiente apartado.

2.- Menú oculto RBS (engineering menu) en los motorola GSM.

Para activar este menú oculto en los teléfonos motorola hay que hacer lo siguiente:

Solo hay que poner en la pantalla principal [][][]113[]1[] para activar el menú o [][][]113[]0[] para desactivarlo. [] significa pausa, y se consigue pulsando asterisco (*) hasta que sale el cuadradito en la pantalla.

Es muy simple en cualquier modelo de Motorola con la versión de

Hardware/Software que no esté en cursiva negrita, funcionarán estos códigos, en los que estén, solo funcionará el RBS Eng field options.

MODELOS:

Tipo Teléfono	Versión Hardware/software Funciona *No funciona*
TX 770	5.3 / 2.3,
d460	***2112***
6200	***1.5 / 1.6*** **,** 1.5 / 1.7 , 3.1 / 1.7 , ***4.0 / 1.9***
7500	5.0 / 2.1 , 5.3 / 2.1 , 5.3 / 2.3 , ***5.4 / 2.3*** , 6.0 / 2.1 , 6.3 / 2.3
8200	***1.4 / 1.3 , 1.4 / 1.5 , 1.5 / 1.9*** , 1.6 / 1.7, ***1.6 / 1.9 , 1.7 / 1.9 , 3.1 / 1.9***

Mas adelante veremos como activar otros menús bastante interesantes, pero ahora vamos a centrarnos en describir esta opción del menú del motorola:

· Active Cell:

Muestra que canal en BCCH (Broadcast Control CHannel) es recibido y te deja ver RxLev, RxLevAM, NCC, BCC, MSTxPwr and C1.

Durante una llamada puedes ver las opciones: RxLev, RxLevFull, RxLevSub, RxQualFul, RxQualSub, Timeslot, TimeAdv, PwrLev

El ActCh (Active Channel(Canal activo)) debe poner "Hopping" durante una llamada. Esto es opcional para el operador de red y puede darnos algunas ventajas. El “hopping rate” es 217 hops/segundos el cual corresponde a un Hop por fracción TDMA (Time Division Multiple Access).

Cuando comunicamos con el BTS podemos ver que clase de SDCCH (Standalone Dedicated Control CHannel) la negociación toma lugar en el DCCH (Dedicated Control CHannels) es usado para registrarse, actualización de localización, autenticación y setup de la llamada .Este canal puede ser mapeado de cuatro maneras diferentes: SDCCH8 si lo combinamos en off y SDCCH4 se combina en on., ver combinación abajo .

· Adjacent Cells:

Te deja ver las caracteristicas que afectan a los 6 repetidores más cercanos (1 - 6) y ver la localización de esos canales. Presionando (OK) te dejará ver diferentes parametros pertenecientes al repetidor seleccionado: RxLev, BCCH decode status (see below), RxLevAM, MSTxPwr, C1,
NCC & BCC.

· System Parameters*:*

Muestra los siguientes datos: Combined, AcsClas, MCC, MNC, LAC, CellID, T3212, BS-PA-MFRM and XZQTY.

Mientras estás realizando una llamada podrás ver además estos menús: Combined, DTX, MCC, MNC, LAC, CellID

Key to the readouts:

ActCh : GSM-900 tiene 124 canales y DCS-1800 tiene 374. Los canales son diferentes con respecto a los operadores – Aquí vemos como se hace en Dinamarca.

Combined*:* *off* usa SDCCH8 y *on* usa SDCCH4. Los canales lógicos pueden ser mapeados con diferentes TIMESLOTS-

Off: BCCH, CCCH y SDCCH esta en otro timeslot, On: BCCH, CCCH y SDCCH están en Ts 0 (Timeslot 0)

AcsClas : Access Class – No estoy seguro de para que se usa.

RxLev: La fuerza de recibimiento de la señal BCCH (000 to 127 dBm), normalmente entre -55 y -90 – la señal cae a RxLevAm *

RxLevAm: Rx Level Acceso minimo – La fuerza de la señal Rx es normalmente alrededor -100 dBm y -110 dBm)

BCC: Base-station Color Code (0 hasta 7)- Es usada para distinguir los repetidores vecinos en el mismo BCCH unos de otros.

NCC: National Color Code (0 hasta 7)

MSTxPwr: El maximo nivel de salida de la MS (Mobile Station) está permitido para acceder a él RACH (Random Access CHannel)- Esto significa que aunque tu pensaras que tu tenias un terminal de 8 Wattios, no siempre te está permitido a emitir a esa potencia.- Mirar las notas en power control abajo.

C1 = (RxLev-RxLevAm-MAX((MSTxPwr-MSMaxRxPwr),0)) Esto es calculado y enviado a la BSC (Base Station Controller) Que usa este criterio para decidir cuando hacer un handover. C1 es mas útil que RxLev, desde que MSTxPwr & MSMaxTxPwr estás dentro de una cuenta. **MSMaxTxPwr** es la potencia máxima de salida en dBm (para GSM normalmente 33 pero 39 con el kit de coche).#

RxLevFull C1 valor con continua transmisión desde el repetidor #

RxLevSub C1 valor con discontinua transmisión desde el repetidor #

RxQualFull Rango de error en un bit con continua transmisión desde el repetidor #

RxQualSub Rango de error en un bit con discontinua transmisión desde el repetidor #

Timeslot : El actual timeslot (0 hasta 7 - TDMA permite ocho canales para ser acomodado dentro de una RF carrier)

TimeAdv TA (Timing Advance) (0 hasta 63) - TA puede ser multiplicado por 547 metros (35 km) para obtener la distancia de la base emisora BTS

PwrLev: Muestra en que nivel de salida de la señal está emitiendo el teléfono - (mirar abajo en la sección de power control) #

DTX: función de transmisión discontinua para ahorrar bateria o para hacer mas fluido el trafico de la red.

MCC: Mobile Country Code 214 = España

MNC: Mobile Network Code 07 = Telefónica, 01 = Airtel)

LAC: Local Area Code (a.k.a. LAI), muchos repetidores contienes el LA(Local Area). El tamaño del área es variable y definible por el operador. A LU (Location Update) debe coger lugar en la MS y dejarlo en la LA. El LAC es de 2 bytes de largo y toma valores entre 0 y 65535.

CellID: Un único número que identifica el repetidor activo.

T3212: Horas entre la actualizaciones periodicas del LU. El Location Update Timer es mejor como HLR (Home Locaton Register) timeout. Si un teléfono pierde la cobertura y no tiene oportunidad de mandar un "IMSI Detach" (para hacer un log off), entonces el teléfono será paginado en el ultimo lugar de la LA, la cual deberá forzar *a)* en los canales de radio y b) entre el BTS, el BSC (Base Station Controller) y el HLR.

BS-PA-MFRM :???? 9 para 238-01 & 8 para 238-02 repetidores-poder de amplificación ??? (un powerlevel ?)

XZQTY : ???? 14.3 para 238-01

Reception Status:

BCCH decode status	Explicación
Not Synced	La estación móvil no está sincronizada con la estación repetidora y no puede dar Timeslot para otra.
No FCB	La Frecuency Correction Burst no se encuentra. El FCB está en la Frequency Control Channel que es asignada a todos los otros TimeSlot 0. El FCB tiene una longitud de 142 bits, pero no llevan información, solo identifica al FCCH y permite la sincronización del canal al ser

	encontrado en el siguiente TimeSlot 0.
FCB Detect	El FCB fue detectado en FCCH, ahora el SCH puede ser encontrado en el TimeSlot 0
SCH Decode	El Synchronisation-burst que tiene una longitud de 64 bits, secuencia de entrenamiento fue encontrada y la información del SCH fue decodificada. El SCH tiene 78 bits y esta cantidad acarrea datos del NCC y BCC
BCCH Decode	Toda la información en el Broadcast Control Channel fue descodificada. Esto incluye el SCH & FCCH, CellID y otros muchos tipos de datos.

· Cuando comparéis los RxLeV, recordar la naturaleza logarítmica de la escala en dB y esta señal de intensidad decrece por un factor 4 cuando la distancia con la BTS es doblada; la señal caerá 6 dB cuando la distancia sea doblada.

Power Control.

Para minimizar las interferencias entre canales y conservar la cobertura, ambos, los móviles y los repetidores operarán al mínimo nivel de fuerza de salida pero manteniendo una calidad de la señal aceptable.
El Power Level puede ser escalonado hacia arriba o hacia abajo en escalones de 2 dB, desde el pico máximo hasta el mínimo de 13 dBm (20 miliWattios) usa está tabla para traducir entre dBm , PwrLev y Power Level. El verde indica un rango para móviles de 2 Wattios.

Power level	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
dBm	43	41	39	37	35	33	31	29	27	25	23	21	19	17	15	13
Watts	20	12.6	8.0	5.0	3.2	2.0	1.30	0.80	0.50	0.32	0.20	0.13	0.08	0.05	0.03	0.02

El menú eng field options ha sido confirmado y denegado en las siguientes versiones (hw/sw):

Phone Type	Hw/sw:El verde indica que el test mode no funciona ·Eng field options
TX 770	5.3/2.3
D460	1.0/1.0,1.2/2.1,1.3/3.6,1.3/3.7
2.500	1.1/2.6
GSM2600	1.5/1.5,1.5/1.6,1.5/1.7,1.5/1.9,2.0/2.1,3.0/1.6,3.1/1.7.3.1/1.9, 3.2/1.9,3.6/1.3,4.1/1.9
DCS 6200	1.6/1.5
6300	1012
7500	5.0/2.1,5.3/2.1,5.3/2.3,5.4/2.1,5.4/2.3,6.0/2.1,6.1/2.1,6.3/2.3,

	6.4/2.4
8200	1.3/1.9,1.4/1.5, 1.4/1.3, 1.5/1.3, 1.5/1.6, 1.5/1.7, 1.5/1.9, 1.6/1.7, 1.6/1.9, 3.1/1.7, 2.1/1.9
8400	1010,1011 (HwSw)
8700/GC87	1010,1210,2011,?2112?,2213,3312,3413,3613(HwSw)

En el proximo numero trataremos sobre lo que nos queda de móviles, y ademas... Explosivos, hacking, y un poco acerca de cómo estafar a T.

Greetings goes to:

Daemon, Freezer, Angelipas, Raptor, Cyberdemon, Seyu, Nati, Tomcat, Ajms, y a todos aquellos que siempre se olvidan.

Cyberhack's Home Page

http://www.geocities.com/siliconvalley/pines/2558