

mexican
revista electrónica underground
hackers
de México para el mundo
mafia

4

☞④④④④④④④ezine④④④④④④④☞

D i s c l a i m e r

Esta revista electrónica fue creada con el único propósito de educar y entretener a la gente. Nosotros en la MHM no nos hacemos responsables del uso que se le dé a la información contenida en ella.

Los textos, gráficas y diagramas publicados aquí, se exponen con el fin de proporcionar datos y material técnico y de investigación mismos que deberán ser empleados siempre con fines educativos.

Contenido

Disclaimer.....	MHM.Staff.....
Introducción	oSUKARu.....
Jugando con el Puerto Paralelo.....	oSUKARu.....
Tarjetas con Banda Magnética.....	Zug.Z.....
Bienvenido a UniNet.....	hkm.....
Telecards de 128 bits (quinta parte).....	El.Narco.....
Micro Procesador Z80.....	Sys_A501.....
PCBs Emulador y Lector de Telecards.....	Brandom.....
Diversión con Alcatel.....	Diente.....
Números escondidos de Telmex.....	hkm.....
Seminario de Programación (ultima parte).....	XROLEX.....
Diagrama de flujo de emulador de Cartman.....	Illan.....
La Mente de un Phreak.....	ShellGhost.....
Despedida.....	oSUKARu.....



Introducción:

Bienvenidos a la cuarta entrega del eZine de la Mexican Hackers Mafia. De nuevo pasó lo que nos había pasado con la primera y la tercera entrega y es que debido a compromisos de trabajo y de los estudios tardamos demasiado en liberarla.

Lo bueno es que ya esta terminada y sinceramente es la mejor entrega de la revista hasta ahora según mi punto de vista, tenemos excelentes textos y tutoriales como es el de programación del micro Z80, también tenemos textos de Illan, de hkm y de Zug y de muchos otros.

En este numero tenemos la ultima parte del curso sobre T2G de el Narco, y el ultimo capitulo del seminario de programación de XROLEX.

Quiero aprovechar a felicitar a Miguel Guillén Hdz, cuyo logo fue el ganador de nuestro concurso para crear la portada del cuarto eZine. También mando un saludo y agradezco a todos los que nos hicieron el favor de mandarnos sus logos para concursar.

Los dejo para que disfruten de esta revista, espero que les guste tanto como a nosotros.

--oSUKARu--



Jugando con el Puerto Paralelo

Por: --oSUKARu--

¿Que les parecería poder prender y apagar su TV, la luz de su cuarto, un pequeño robotsito, el estereo, etc, desde la comodidad de su silla preferida utilizando la computadora?

¿Les suena chingón? ¿Algo complicado que solo "geeks" pueden hacer y eso en películas quizás? Pues en realidad es más fácil de lo que parece y hoy les explicaré como.

Primero, es recomendable que tengan conocimientos de electrónica y de algún lenguaje de programación, aunque no esencial.

Materiales a emplear:

- 1 Conector DB25 para cable plano
- 1 Cable plano de 24 hilos
- 1 Conector de cable plano para proto-board
- 1 Proto-Board
- 8 LEDs Color Rojo Difusos
- 8 Resistencias 1k ohm
- 1 ULN2803
- 1 Relevador

NOTA: Antes de que salgas corriendo a la tienda electrónica a comprar los componentes termina de leer el texto, dependerá del tipo de circuito que quieras armar los dispositivos que necesites, puedes emplear más o puedes emplear menos (sigue leyendo y verás por que).

Para empezar les daré un poco de teoría y el pin-out del puerto paralelo:

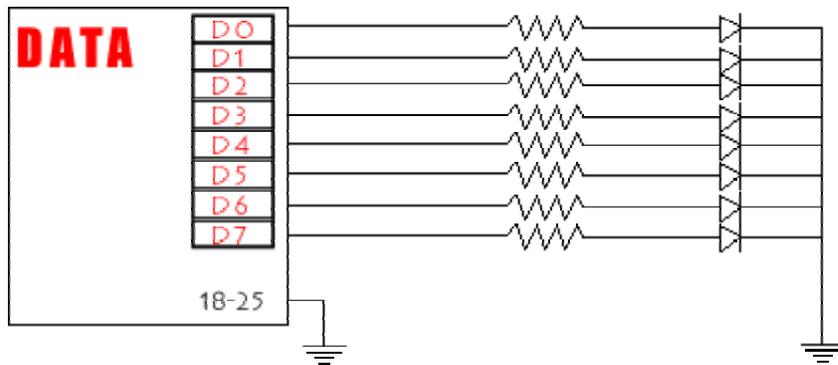
DATA	D0
	D1
	D2
	D3
	D4
	D5
	D6
	D7
CONTROL	C0
	C1
	C2
	C3
	C4
	C5
	C6
	C7
STATUS	S0
	S1
	S2
	S3
	S4
	S5
	S6
	S7

D0	DATA 0	2	SALIDA
D1	DATA 1	3	SALIDA
D2	DATA 2	4	SALIDA
D3	DATA 3	5	SALIDA
D4	DATA 4	6	SALIDA
D5	DATA 5	7	SALIDA
D6	DATA 6	8	SALIDA
D7	DATA 7	9	SALIDA
C0	STROBE	1	BIDIRECCIONAL
C1	LINE FEED	14	BIDIRECCIONAL
C2	INITIALIZE	16	BIDIRECCIONAL
C3	SELECTION	17	BIDIRECCIONAL
C4			
C5			
C6			
C7			
S0			
S1			
S2			
S3	ERROR	15	ENTRADA
S4	SELECT	13	ENTRADA
S5	PAPER END	12	ENTRADA
S6	ACK	10	ENTRADA
S7	BUSY	11	ENTRADA

Como pueden ver por el pin-out, es obvio que en un principio no se pensó en que el puerto hiciera nada más que servir como interfaz entre la computadora y la impresora. Inicialmente se diseñó por la compañía Centronics exactamente para ese propósito, pero gracias a los hackers y los hobbistas electrónicos hoy en día lo podemos emplear para mucho más que eso.

Las líneas que se encuentran en "negritas" significa que están negadas, es decir que en lugar de esperar un 1 lógico para saber que la condición es verdadera, esperan un 0. (Si no entiendes y quieres saber sobre electrónica digital lee el artículo para principiantes de la eZine 1).

¿Qué les parece si para entretenernos un rato hacemos un circuitillo que prenda y apague LEDs? Bien, aquí está el esquema para que lo hagan en el proto:



Momento, casi se me olvida explicarles como hacer el cable para el puerto paralelo :P

Bueno suponiendo que aun lo han armado así se hace: Tenemos el cable plano que es de 24 pines y el DB25 es de 25 (apoco :), ¿Qué pin dejamos fuera? Bueno pues del 18 hasta el 25 son puras tierras, así que simplemente pondremos un pequeño puente entre una de ellas y el pin que queramos dejar fuera. Listo, solo es cuestión de colocar el cable plano sobre ambos conectores, apretar con un chingo de ganas y quedará listo para usarse. (Recuerda poner el cable rojo en el pin 1 para que sepas bien como va el asunto).

Ahora si, a divertirnos con los LEDs, ya tienes tu cable, ahora solo es cuestión de hacer el circuito en el proto-board (esos son LEDs no diodos, se me olvido ponerles las flechitas de la luz y me da hueva editar el dibujo así que así lo dejo).

Para mandar un 1 lógico a la salida puedes hacerlo con varios lenguajes de programación, con Pascal se utilizaría *portw[]* o *port[]*, pero como a mi lo que me gusta es ensamblador, lo vamos a hacer todo a pie:

Primero necesitas saber en que dirección tienes el puerto paralelo. Para esto, abre una ventana con MS-DOS y escribe *debug* entraras al editor de ensamblador. Ahora escribe ' D 0:408 ' (sin las comillas claro) te aparecerán una serie de números como se ve en la figura:

```

C:\WINDOWS>debug
-d 0:408
0000:0400          78 03 00 00 00 00 00 00          x.....
0000:0410  23 C4 00 80 02 80 00 20-00 00 26 00 26 00 34 4B  #.....&.&.4K
0000:0420  30 52 38 48 0D E0 67 22-0D 1C 64 20 20 39 34 4B  0R8H..g".d 94K
0000:0430  30 52 38 48 E0 4B E0 4B-E0 4B 30 52 3A 34 00 80  0R8H.K.K.K0R:4..
0000:0440  00 00 C0 00 00 00 00 00-00 03 50 00 00 10 00 00  .....P.....
0000:0450  00 0C 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....>0.>.....
0000:0460  0E 0D 00 D4 03 29 30 A4-17 29 85 FF 9E B8 12 00  .....>0.>.....
0000:0470  00 00 00 00 00 00 01 00-00-14 14 14 3C 01 01 01 01  .....<.....
0000:0480  1E 00 3E 00 18 10 00 60          ..>....

```

Los primeros dos pares de numero indican la dirección del puerto, así que ahora sabemos que se encuentra en el 0x378h (recuerda que los procesadores Intel trabajan con formato little endian)

Ahora sacaremos un 1 por alguna de las salidas para prender un LED.

```
-O 378, 02
```

Tendremos que tener un LED prendido ahora. Cambia el 02 por un 00 y lo apagarás.

Pero yo no quiero estar metiendome al fastidioso debug cada que quiera prender algo, ¿Qué hago? Pues es hora de entrar a la programación. Escoge el lenguaje que se te guste y aprende como manejar el puerto paralelo, o utiliza este pedazo en ensamblador (en Pascal, C, C++ y varios otros lenguajes puedes meter ensamblador en línea).

```
MOV DX, 378h          <---- Mueve a DX el valor en el que esta el PP
MOV AL, 02            <---- Pon el Numero que quieres encender (BDC)
OUT DX, DL            <---- Saca el valor por el Puerto.
```

Algo que se me olvidaba mencionar es que la salida del puerto se maneja en BCD, es decir el byte lo divides en dos nibbles y trabajas con cada uno por separado.

Ahora que ya tienes esas instrucciones puedes hacer un programa más chingón como una serie de luces con los LEDs (recuerda meter un retardo después de cada que mandas el pulso por el puerto o no veras que cambio).

El código quedaría así:

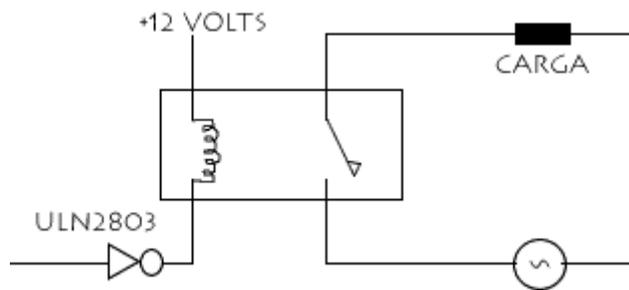
```
MOV DX, 378h
MOV AL, 02
OUT DX, DL
retardo
MOV DX, 378h
MOV AL, 18
OUT DX, DL
retardo
...
etc...
```

¿Pero que pasó, yo creía que me ibas a enseñar como prender TVs, Estereos, en fin cosas más chingonas, solo vamos a prender foquitos? No, pero si ya sabes prender y apagar LEDs no tendrás problemas en prender la cochera eléctrica de tu casa o las luces del patio, lo único que necesitas son dispositivos actuadores que te permitan hacerlo.

¿Recuerdan el ULN2803 y el relevador que les mencione en la lista de materiales? Pues estos van a ser nuestros acutadores. Los necesitamos porque el PP no puede suministrar mucha corriente, y tan solo nos dará 5 Volts de Corriente Directa, lo que no nos sirve para prender algo como un motor de pasos o las luces de la casa.

Estos dispositivos pueden ser remplazados por TRIACS, SCRS o algun buffer no inversor, todo depende de lo que queramos hacer y como lo queramos hacer.

Entonces el circuito para conectar algo más pesado quedaría así:



Al mandar un pulso al ULN la corriente fluirá hacia el extremo negativo y activará el relevador, cerrando el circuito y prendiendo el aparato.

Por ultimo, el pin-out del ULN2803 lo pueden encontrar fácilmente buscando en google, de cualquier forma, va así: del pin 1 al 8 son las entradas del buffer inversor, del 11 al 18 las salidas, la pata 10 es VCC y la 9 es GND.

Ok, aquí terminamos esta guía practica de cómo utilizar el puerto paralelo para prender y apagar mil cosas alrededor de la casa. Los conocimientos básicos aquí están, solo es cosa de que utilicen su inventiva y creatividad para llevarlo hasta lo extremo. Y recuerden presumir sus avances en el foro de electrónica de la página.

¡Diviértanse!

--oSUKARu--

Mexican Hackers Mafia 2002
<http://www.mhmpbreak.da.ru>

Tarjetas con Banda Magnética

Zug

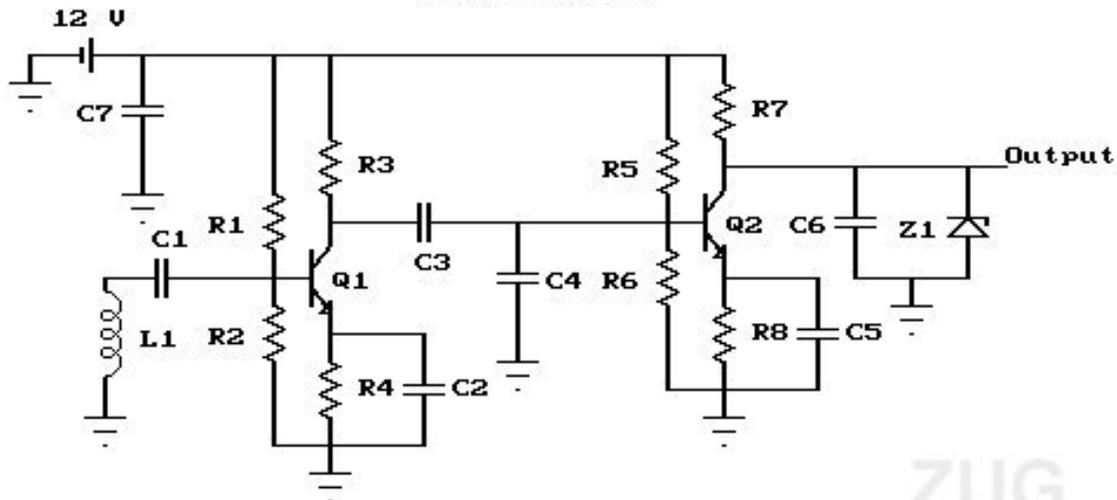
Quien no tiene una tarjeta, de crédito, de debito y hasta unas que no tienes la menor de para que sirve pero tienen una banda negra atrás, pues vamos a ver que tienen, lo que necesitaras son una cabeza magnética, dos transistores, algunas resistencias ya capacitores, una fuente de poder de 12 Volts, un voltímetro y osciloscopio sobre todo en la fase de prueba.

Ahora bien, la cabeza magnética la puedes conseguir de la grabadora de tu hermano, esa vieja mono-aural, que son un poco mas pequeñas de lo que se requiere pero funcionara, te recomiendo no uses una estereo a menos que quieras leer dos tracks al mismo tiempo.

La señal que obtendrás de pasar la cabeza por la banda es muy débil, así que tendrás que amplificarla para poder meterla a la computadora. Por esa razón debes fabricar el circuito.

Amplificador - Lector

Luis Padilla



R1 = 68 k, R2 = 10 k, R3 = 22 k, R4 = 2.2 k

R5 = 8.2 k, R6 = 1 k, R7 = 2.2 k, R8 = 47

C1 = 22 uF, C2 = 10 uF, C3 = 47 uF, C4 = 22 nF

C5 = 150 uF, C6 = 22 nF, C7 = 2200 uF (16 V)

L1 = Magnetic head

Z1 = Zener diode with breakdown voltage around 6 V

Q1, Q2 = Any bipolar silicon NPN general purpose transistor

Donde el Q1 actúa como un preamplificador, incrementando la débil señal abajo de 1mV. Como preamplificador tiene un factor de ruido bajo por el transistor en una carga baja (- 1mA) y voltaje bajo (- 2V)

El transistor Q2 actúa ya como amplificador para la entrada a la computadora, es por eso que la salida se conecta directamente al puerto sin ningún capacitor, así que el voltaje DC tendrás que ajustarlo a las especificaciones del puerto que uses. Q1 y Q2 deberán ser transistores

NPN bipolares de propósito general. El valor de los componentes no es crítico así que usa los que mas se acerque a los valores del diagrama.

El circuito esta diseñado para trabajar con una fuente de alimentación de 12V para lo que te recomiendo uses una fuente de PC, en otro caso cambia el valor de las resistencias para alimentar correctamente los transistores.

Para un mejor desempeño se recomiendo que las resistencias R2 y R6 fueran variables con valores de 20 y 2 K respectivamente, centrándolas para tener al rededor de 10 y 1 K, entonces pasa por la banda y cambia R2 hasta que tengas la mayor amplitud y el menor ruido posible, en este momento te ayudara mucho el osciloscopio, pero como no todos tenemos uno en casa, pues ahora usa la bocina de tu PC y ajusta con el sonido, tienes que pegar la oreja.

Una vez que R2 esta en su desempeño optimo, ajusta R6. Usa el Voltímetro para medir el DC a la salida del circuito. No pases ninguna tarjeta hasta que el DC de salida este entre 4 y 4.5 V. Asumiendo con esto que usaras el valor TTL del puerto de la computadora que debe ser +5v, pero como el amplificador al momento de leer una tarjeta incrementara su voltaje, es posible que pasara los 5v por eso ajústalo abajo de este valor.

El diodo zener Z1 se una protección para el puerto de la computador en caso de un incremento en el voltaje pudiera dañarlo, debe ser entre 5.5 y 6.5v en caso de que no tengas zener puedes usar normales como es acostumbrado y/o bajar el CD al rededor de 3.0 a 3.5v para obtener algo de protección.

Debes poner atención al aterrizar cada parte del circuito, especialmente con altas frecuencias, esa es la función de los capacitores C4 y C6. Otro dato importante es aterrizar correctamente el shield de la cabeza y tratar de conectarla los cables mas cortos que sea posible para evitar el ruido.

Para leer correctamente las bandas magnéticas existen dos métodos, pasar la cabeza por la banda o la banda por la cabeza, selecciona el que mas te acomode pero aun cuando la segunda suena mas fácil la primera ofrece reales ventajas para cuando hagas el copiador de tarjetas.

Este lector debe conectarse a el puerto paralelo con la salida del lector al pin no 15 y aterrizado en el pin No 18, también puedes conectarlo en el puerto de Joystick en el pin No 2 y aterrizado en el 4.

Por ultimo usa el compila este programita viejo o modifícalo para actualizarlo a la nueva era!

Recuerda leer tarjetas puede ser muy útil, para conocer lo que dicen, para poner una cerradura a tu casa con este lector, para muchas cosas, claro que menos para lo que tu estas pensando, creo que eso si es ilegal ; -)

Programa de Luis Padilla (Magnet.c -adjunto en el zip-)

Bye.

Zug



```
#####
#                               #
# Bienvenido a UniNet          #
#                               #
#                               #
#                               #
#                               #
#####
```

1234567890123456789012345678901234567890

Hola. Este pequeño texto esta dedicado a todas las personas* que por el constante interés en el hacking y phreaking dentro de México mantienen el underground vivo.

Desde hace mucho tiempo la gente pensaba que Prodigy / Telmex tenían una forma en la que pudieras conectarte sin tener que pagar la llamada. Algún tipo de 01-800 o algún prefijo secreto.

El pasado 07/ABR/02 encontré un terminal de UniNet al marcar el siguiente numero: [*][1][2][3][4][5][6][7][8] Esto funciona en una terminal TTY y pide login y passwd los cuales son los mismos que tu conexión de Prodigy.

Después de comprobar que funcione dentro del Estado de México, Mérida, Monterrey, Quintana Roo y el D.F. Empecé a realizar este texto.

Saludos a todos, espero estén bien.

hkm
Miembro: <http://www.hakim.ws>

Aquí vienen los Shouts...

```
**TEAM SHOUTS*****
*Acid Klan - www.acid-klan.org      *
*Hackers Mexico - www.hackers.com.mx *
*Hakim.ws - www.hakim.ws           *
*MHM - www.mhmpbreak.da.ru         *
*Raza Mexicana - www.raza-mexicana.org *
*****
```

```
**SHOUTS*****
*CronD, Taer, K7 y todos los olvidados *
*****
```

Tarjetas Argentinas T2G
Por: El Narco

- CAPITULO V -

Operación WRITECARRY: (*Transporte de escritura*)

Que carajo es el writecarry???, se preguntarán muchos...

El writecarry es como si fuera una doble escritura.. pero a diferencia del write esta operación debe poner al siguiente byte todo a unos, es decir a FF.

La secuencia es como sigue a continuación:

1 - La cabina se posicionara en un bit no escrito.

2 - Luego la cabina realizará la grabación poniendo a 0 el bit que estaba a 1. Es como si fuera una **Operación WRITE**, es decir **RST** se pone en nivel alto mientras que **CLK** permanece bajo, después **RST** baja.

3 - **CLK** se eleva por un mínimo de 10ms mientras **RST** permanece bajo, y en ese momento es cuando pasamos a 0 el bit que esta a 1. Y ahora viene lo que se trata el writecarry.

4 - **RST** es puesto a 1 nuevamente mientras **CLK** permanece bajo para deshabilitar el incremento del siguiente bit, luego **RST** baja.

5 - **CLK** se eleva por un mínimo de 1ms, mientras **RST** permanece bajo para escribir el siguiente byte todo a, 1 es decir a FF como hemos explicado anteriormente.

6 - Luego de esto, volvemos a la dirección anterior, volvemos al bit que fue grabado, esperamos que baje **CLK**, y luego saltamos a **CLK** para seguir leyendo...

Para tenerlo mas claro:

Por ejemplo tenemos los siguiente bytes

```
00000000 x4096
00000000 x512
11111111 x64
00000000 x8
00000000 x1
```

El valor de estos bytes para la cabina vendría siendo \$ 5,12

Cuando la cabina se posiciona en el bit 7 del contador octal x64 intenta grabar ese 1 y pasarlo a 0 es decir, sube RST, baja RST , sube CLK, grabamos ese bit es decir lo pasamos a 0, baja CLK, ponemos un 0 en I/O

```
00000000 x4096
00000000 x512
01111111 x64
00000000 x 8
00000000 x1
```

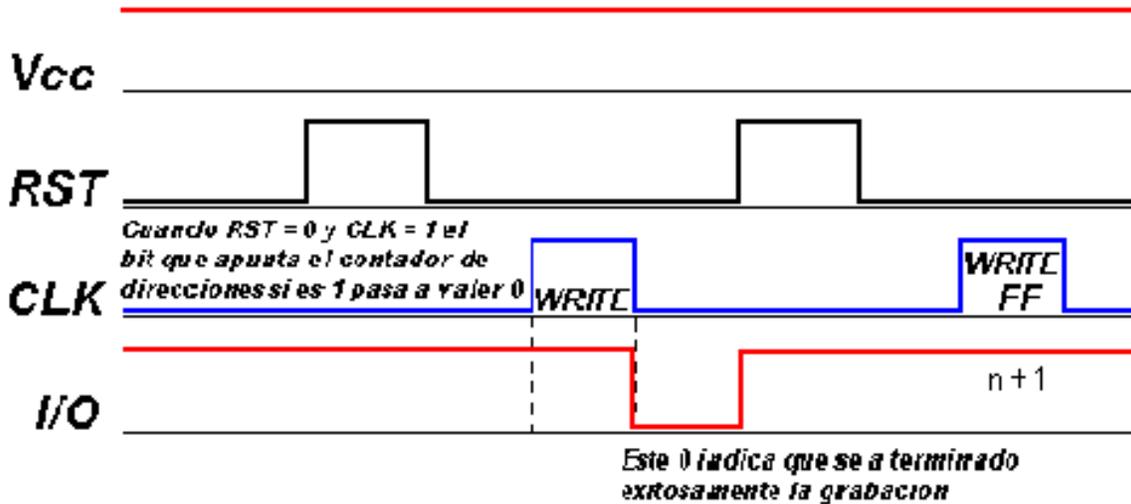
y si la cabina intenta hacer un writecarry, lo haría de esta manera (Acuerdensen que el writecarry lo va hacer en el bit que grabamos con anterioridad, es decir el bit 7 del del contador octal x64).

Sube RST, baja RST, sube CLK, incrementamos la dirección (es decir la dirección que le sigue a la que estamos), grabamos FF en la dirección incrementada, luego volvemos a la dirección donde

estábamos al principio y nos posicionamos de vuelta en el bit que fue grabado (el bit 7 del contador octal x64), entonces nos quedaría de la siguiente manera

```
00000000 x4096
00000000 x512
01111111 x64
11111111 x8
00000000 x1
```

La secuencia gráfica



Ensamblando:

En nuestro programa como lo haremos ???

Yo lo realicé en la rutina principal, la de RESET, básicamente esta rutina es la más importante de todas, por que desde ahí derivamos a todas las demás.

Y como lo hice ???, de la siguiente manera:

```

;***** RUTINA DE RESET *****
RESET          btfss  PORTB , 0      ; Subió RST ???
                goto   RESET        ; No, seguimos esperando
                bcf    PORTA , 4     ; Si, limpiamos la salida
ESPERAR_CLOCK2 btfsc  PORTB , 7     ; Subio clock ???
                goto   RESETEAR     ; Si, reseteamos principalmente
                btfsc  PORTB , 0     ; Bajo RESET ???
                goto   ESPERAR_CLOCK2 ; No, seguimos esperando
                btfsc  EEDATA , 7   ; Leemos el bit 7 de EEDATA
                bsf    PORTA , 4     ; El bit 7 es un 1 y lo sacamos por I/O
                btfss  OPCION , 0   ; Es Write o WriteCarry ???
                goto   WRITE        ; Es WRITE
                goto   WRITECARRY   ; Es WRITECARRY

;***** FIN DE LA RUTINA RESET *****

```

Esto lo he explicado básicamente en el capítulo anterior, pero a este programita le he agragado unas instrucciones.

1 – OPCION:

Este es un registro definido en otra dirección de memoria realizada por mi, este registro lo empleo para saber si es write o writecarry. Hagamos de cuenta que la cabina realizó una Operación Write y en nuestra operación debemos poner el registro OPCION a 1 (bsf OPCION , 0) por si la cabina intenta grabar nuevamente sobre ese mismo bit, entonces pregunta si OPCION esta a 1, si esta con ese valor saltamos a la Rutina de WRITECARRY.

```
;***** RUTINA WRITECARRY *****  
  
WRITECARRY    btfss    PORTB , 7      ; Subio CLOCK ???  
              goto     WRITECARRY ; No, seguimos esperando  
              movf     EEDATA , W ; Retenemos el valor de EEDATA para recuperarlo  
              movwf    RETENER      ; mas tarde  
              movlw   0xFF          ; W se carga con el valor FF  
              movwf    EEDATA       ; EEDATA se carga con el valor FF  
              incf     EEADR , F    ; Incrementamos el contador de programa  
              GRABAR      ; Escribimos FF en la direccion incrementada  
              movf     RETENER , W  ; Recuperamos el valor  
              movwf    EEDATA       ; antes del writecarry  
              decf     EEADR , F    ; Volvemos a la dirección de antes  
              clrf     OPCION      ; Limpiamos opción de writecarry y grabar  
  
ESPERAR_CLK   btfsc    PORTB , 7      ; Bajo CLOCK ???  
              goto     ESPERAR_CLK ; No, seguimos esperando (PCL-1)  
              goto     CLK         ; Esperamos clocks  
  
;***** FIN DE LA RUTINA WRITECARRY *****
```

Cuando entramos en esta rutina lo primero que hacemos es verificar si CLK se levantó, si no es así esperamos a que esto suceda, una vez que esto ocurre debemos retener el valor de EEDATA para luego volver a esa dirección una vez completado las siguientes grabaciones.

Incrementamos la dirección a la que estábamos y ponemos FF en dicha dirección a través de la rutina GRABAR (ver capítulo anterior). Luego decrementamos la dirección y volvemos al byte que fue retenido, borramos el registro OPCION, y esperamos que baje CLK para luego volver a leer los siguientes bytes.

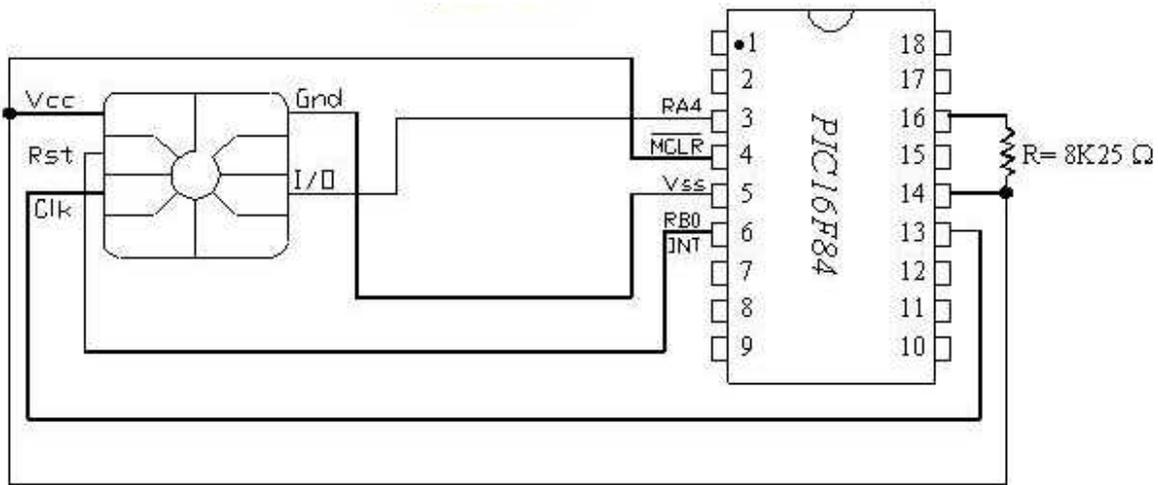
Bueno, al parecer he terminado de definir como se compone una tarjeta de esta generación. Espero haberles aclarado sus dudas e ideas, ahora pasemos a la parte que seguramente les interesa a todos.

El Emulador

Seguramente te has pasado por alto todo lo escrito anteriormente para ver si puedes conseguir un emulador funcional, lamento desilusionarte, he decidido NO exponer mi emulador por el simple motivo de que yo no me rompí la cabeza pensando y estudiando para que tu vengas y te armes la tarjeta sin saber nada. Pero si has leído, comprendido y has seguido paso a paso lo que desarrollé a lo largo de estos capítulos, entonces ya estás orientado para diseñarte tu propio emulador. Lo que escribiré en las siguientes líneas son algunas pistas para que logres dicho objetivo (esta es mi forma de ver, lo que significa que no sea la única manera de lograrlo).

El Circuito

El conexionado es básicamente como el que tiene todo el mundo. Por que todo el mundo ??? En realidad es una larga historia, pero voy a sacarles la intriga en las próximas cuatro líneas. Hace un par de años un grupo muy reducido se encontraba en el foro de AAS, (Yo incluido) debatiendo, discutiendo y experimentado la emulación de estas tarjetas, entonces se llegó a un acuerdo para que todos sigan el mismo camino, y ZACKY en su ya inexistente página expuso esta forma de conexión.



1 - La ventaja de esta forma es que podemos usar interrupciones, yo en mi caso y la de muchos otros utilicé la interrupción por activación de la puerta RB0 / INTE que esta conectada a la patilla RST, entonces cada vez que se produzca un nivel alto en dicha puerta se ejecuta la rutina RESET.

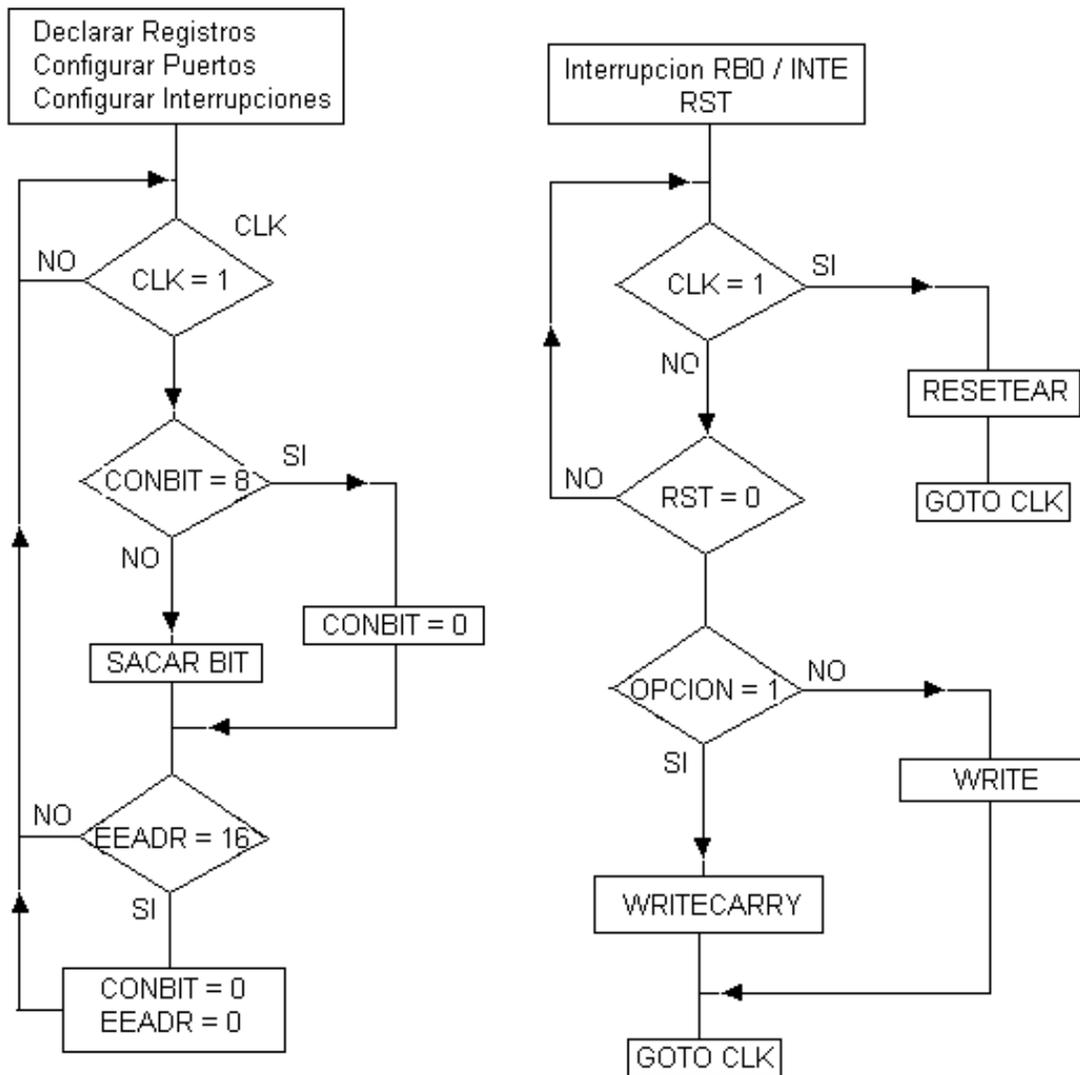
2 - La Puerta RA4 se emplea para la salida de datos I/O.

3 - CLK esta conectada a la puerta RB7, en esta puerta también se puede realizar interrupciones por cambio de estado de las puertas RB7 – RB4. Pero yo este tipo de interrupción no lo he empleado.

4 – También se utiliza una oscilación del tipo RC (Resistencia – Condensador), pero ya que la cabina no necesita de una frecuencia tan estable no se utiliza dicho C.

El diagrama de Flujo (Organigrama)

Antes de programar es conveniente realizar una forma de guía para no tener que estar pensando y perdiendo el tiempo para de lo que se tenia que desarrollar.



La Recarga

Básicamente es muy sencilla, se trata de comparar direcciones (La de x512 y la de x64) y si ambas direcciones son 00 saltamos a grabar los valores que deseamos en el contador octal .

La recarga la podemos efectuar antes de que se produzca el RST ya que tenemos tiempo de sobra.

Despedida

He concluido definitivamente este estudio, con este ultimo documento doy por finalizado el paseo por este mundillo, ahora voy a derivar a otras cosas como es la clonación de celulares, tarjetas para DIRECTV o SKY o a las tarjetas magnéticas.

Saludos..... ;oP

Archivos Recomendados

- **EmuEstudioTT.zip**
- **Tarjetas de 128bit por Wolfhack**
- **Lector THE ELECTRÓN 3.0**
- **Lector Emultronix (ARGOT)**

“ No me responsabilizo del uso ilegal de los datos aquí expuestos, este documento ha sido desarrollado únicamente para uso experimental ”

Agradecimientos

Sinceramente debo agradecer a todas aquellas personas que se iniciaron a partir del foro de AAS y sus derivaciones ZACKY, DARKEB, MURDOCKDJ, SHELLGHOST, JMB4U, DARKMAN2010 y otros que no recuerdo, en su mayoría comunidad española, que realmente tengo un muy buen concepto del poder de imaginación que tienen, no voy a empezar a decir quienes son por miedo a olvidarme de alguien, ustedes sabrán.

También a los canales #Gabinas y #Comunica2 del IRC Hispano donde se encuentran todo los “GROSOS” de este mundillo.

Agradezco al grupo **Mexican Hackers Mafia** por publicar mis documentos en su ZINE.

Nota

Cualquier error por favor comunicarse a: tecnicoinforma@yahoo.com.ar

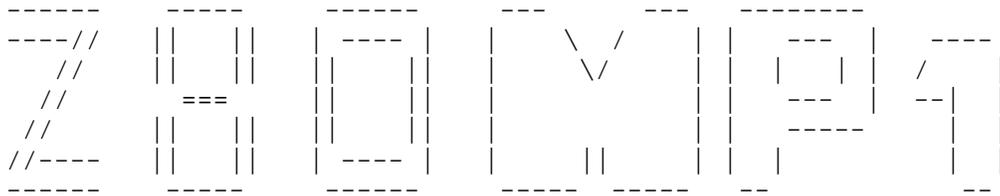
Este documento puede ser editado en cualquier página web siempre y cuando respeten el contenido y a su autor.

Autor : PitufoEnrike

País : MENDOZA – ARGENTINA

Creado el : 22 / 11 / 2001

Sitio Oficial : <http://www.tecnicos.da.ru>



Por: Sys_A501
para: Nazgul Clan y MHM

.....
Introducción:

Y que diablos es Z80??. Pues el Z80 es un Micro Procesador de 8 bits de la marca Zilog... 8 bits son 8 dígitos binarios que pueden tomar 2 valores, 1 o 0, como ejemplo tenemos este número:

Binario	10011010
Decimal	154
Exadecimal	9AH <-- La "H" significa Hex o hexadecimal.

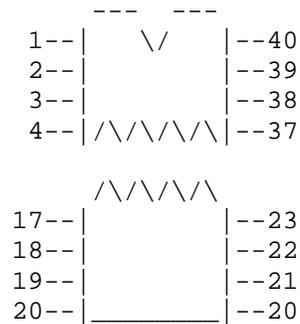
Estos son 8 bits, que equivalen a un Byte; pues bien, como tenemos 8 espacios para combinar "1" y "0", entonces podemos tener 256 combinaciones diferentes, que van del 0 al 255 en decimal, osea 00000000 al 11111111, que en hexadecimal es del 00H al FFH.

Y eso de que nos sirve?. Pues esos 8 bits nos sirven para darle instrucciones a nuestro procesador.

¿Cómo se hace eso?. Depende del circuito, puede ser de forma manual o por medio de una memoria, hay que tomar en cuenta que las instrucciones deben de estar en binario, por lo cual hay que repasar esos libros de matemáticas, o tener una calculadora que nos ayude.

.....
Pines, Patitas o Terminales:

Ya se que se siguen preguntando...
Y como se hace eso físicamente?. Pues el procesador tiene 40 patitas, pines o terminales, que no son más que conexiones que tiene el interior del Micro procesador (Mp) con el mundo exterior, cada una de estas patitas, tiene una función específica; dado que no me pienso poner a dibujarles patita por patita, les voy a explicar como se enumeran y la función que tiene cada una de ellas...



Y si no les quedó claro, ponen la marca del Chip apuntando hacia adelante y hacia arriba, y la primer pata de la izquierda es la 1, y la ultima de la izquierda es la 20, la ultima de la derecha es la 21, y la primera de la derecha es la 40...

Significado y funcionamiento de los pines...

(Las flechas al principio, indican si son de entrada o de salida o de los dos...)

(<--- = Salida)

(---> = Entrada)

(<---> = Bidireccional)

Bus de Direcciones:

<--- pines 30 al 40: A0 hasta A10 (la A es de Address)

<--- pines 1 al 15: A11 hasta A16

Bus de Datos:

<--> Pines 14, 15, 12, 8, 7, 9, 10 y 13: son D0, D1, D2, D3, D4, D5, D6 y D7; respectivamente (la D es de Data)

Pines de control de sistema:

(El signo "-" indica que esos pines son activos a nivel bajo...)

<--- Pin 27: M1- Modelo de interrupciones #1

<--- pin 19: MRQ- Requerimiento de Memoria

<--- pin 20: IORQ- Requerimiento de Puerto

<--- pin 21: RD- Read, cuando lee de memoria o puerto, este se activa

<--- pin 22: WR- write, cuando escribe a puerto o memoria, este pin se activa

<--- pin 28: Rfsh- Refresca los datos...

Pines de control del CPU:

<--- Pin 18: Halt- Se activa en espera de una interrupción

---> Pin 24: Wait- Le dice al procesador que espere (lógico verdad...)

---> Pin 16: INT- Interrupción enmascarable, se puede desactivar

---> Pin 17: NMI- Interrupción no enmascarable, esta no se puede...

Pines de control de Buses

---> Pin 25: BUSREQ- Es para pedirle el control de los buses al procesador
 <--- Pin 23: BUSACK- Con este pin, el procesador dice que los buses están libres para ser usados...

Pines de Alimentación:

---> Pin 6: CLK Aquí se conecta el clock o cristal
 ---> Pin 11: +5V El positivo de una fuente de alimentación de 5 Volts de corriente directa
 ---> Pin 29: Gnd El negativo de la misma fuente...

.....
 Registros...

Y que son los registros?. Pues para no meternos en problemas, son pedazos de 8 y/o 16 bits de memoria, que se utilizan como variables...
 Como que variables?. Si, Variables dentro la programación en ensamblador.

Los registros básicos son los siguientes:

Registro	Nombre o Uso	Tamaño en bits	Notas
A	Acumulador	8	Operando, resultados de operación y datos
F	Banderas(Flags)	8	Cada bit, significa algo, sirven de condición
B	Uso general	8	Se puede usar solo (8b) o junto con C (16b)
C	Uso general	8	Se puede usar solo (8b) o junto con B (16b)
D	Uso general	8	Se puede usar solo (8b) o junto con E (16b)
E	Uso general	8	Se puede usar solo (8b) o junto con D (16b)
H	Uso general	8	Se puede usar solo (8b) o junto con L (16b)
L	Uso general	8	Se puede usar solo (8b) o junto con H (16b)
IX	Indexado	16	Usado para direccionamiento Indexado
IY	Indexado	16	Usado para direccionamiento Indexado
SP	Pila	16	Define la pila

Nota:

Cuando se usa la combinación de registros BC, DE y HL; internamente, los datos se organizan así:

Bytes Altos	Bytes Bajos	Registro
B	C	Bc
D	E	De
H	L	Hl

Otra Nota:

Cuando el procesador identifica una interrupción, inmediatamente guarda la dirección de memoria siguiente a la que se encuentra ejecutando y salta a la dirección de memoria 0038H.

Y hasta aquí la 1º parte de Esta serie del Z80, En la siguiente, veremos una parte de la tabla de instrucciones y uno que otro circuito para armar en un Protoboard...

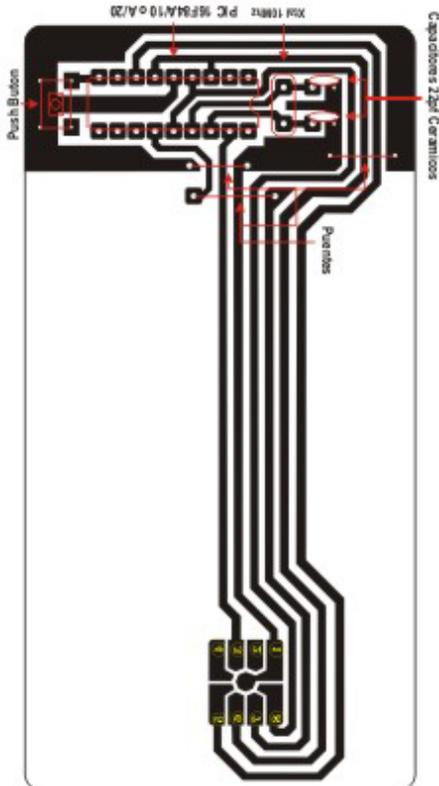
Que por que lo dejo así???... Pues para que sigan esta serie, y no se pierdan ninguna parte...

Sys_A501

Nazgul Clan: nazgul.2ya.com
MHM: mhmpbreak.da.ru



PCB's Emulador y Lector de tarjetas



Antes que nada GRACIAS a los maestros Cartman y Elektron por sus investigaciones y a toda la gente que esta trabajando en este proyecto...

PCB Emulador: Basado en el esquema eléctrico de Cartman, se le dio la vuelta para insertar los componentes por el lado de la fibra (placa circuito), de tal modo que soldemos solamente las patas de los componentes y las de los puentes por el lado del cobre (placa circuito), es por eso que en el dibujo se ve alrevez.

PCB Lector: 2 Versiones basados en los que propone Elektron, el primero se alimenta del puerto paralelo, (Db25 18-25 negativo) y (Db25 5 positivo) el segundo lector se debe ser alimentado por una pila o fuente de energía 5V, al usar este lector debes tener cuidado en la polaridad. Debido a que es muy difícil de conseguir el zocalo Smartcard el pcb incluye el conector para el chip de la tarjeta, para que haga buen contacto con el chip sugiero que se ponga una gota de estaño donde están los números (Cuidado de no "puentear" los contactos) y lijar para que quede al mismo nivel, no olvides poner los puentes.

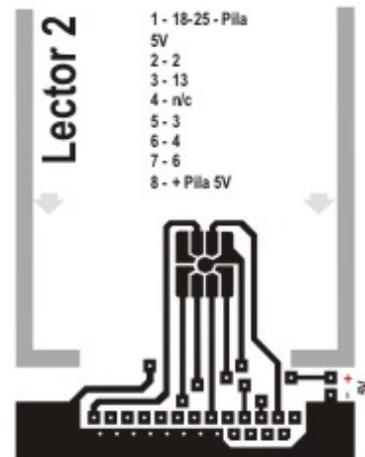
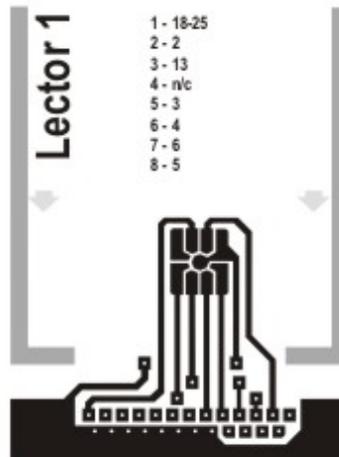
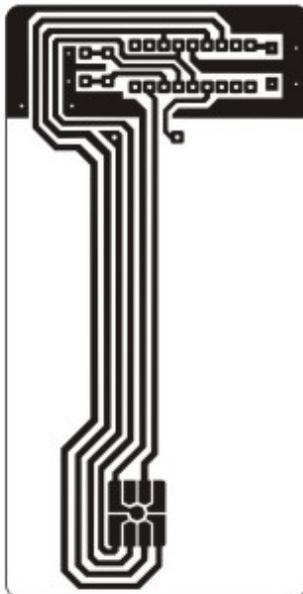
Nota: Para leer el emulador tenderías que poner la cara de cobre contra la cara de cobre del lector, también es importante poner las guías para que la tarjeta entre ajustada y haga un buen contacto.

Hasta ahora no los he probado pero en teoría se supone que funcionan...

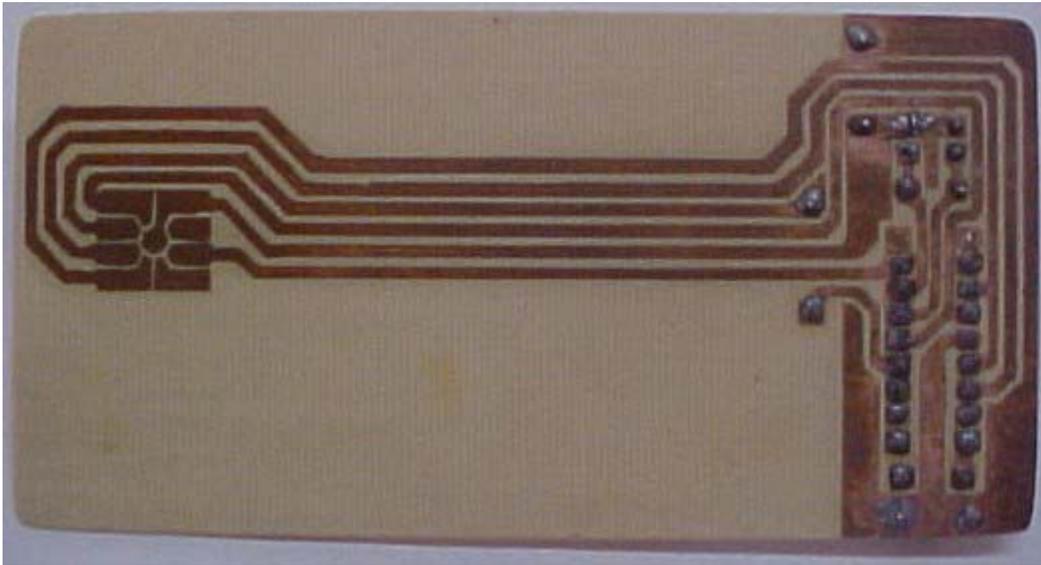
Si tienen algún comentario será bien recibido en... brandom_x@yahoo.com.mx

Salu2 ato2

Brandom X



PCB emulador:



* Diversion con Alcatel *
* Como convertir tu modem Home en una version Pro *

Adaptado de: <http://www.sateh.com/hacks/alcatel.php>

Este documento explica como puedes activar las capacidades PRO de tu modem.

Lo mas interesante que he descubierto hasta ahora es que puedes activar PPP (pero aun no logro conectar el modem en PPP). Teóricamente en el momento en que logremos conectar el ppp no necesitaras el programa obsoleto e inservible de PPTP. Solo necesitaras conectar tu maquina, switch o router y configurarlo directamente, no se si alguno de ustedes intento instalarlo en alguna version de linux que no sea RH 7.2

El modem actuara como un router NAT/PAT que quiere decir que podrás conectarlo a un hub o switch con la cantidad de computadores que quieras en vez de que solo sea 1.

También podras acceder a todas las funciones avanzadas que se supone que solo tiene acceso telmex a ellas, así como el debug.

Todos los cambios son en software.

Disclaimer

Tienes el riesgo de cambiar las configuraciones de tu modem y no tenerlas de regreso a su estado original. diente no se hace responsable por cualquier daño que le puedas hacer a tu MODEM temporal o permanentemente. ESTAS ADVERTIDO!!! DIVIERTETE :)

Paso 1 - Obtener el password en modo experto

Necesitas cambiar una configuración que solo esta disponible en el modo EXPERT del modem.

Este es un modo que esta protegido por un password que podrás conseguir de la siguiente manera.

Hay un dato de informacion "Encriptado" a partir del cual podras conseguir el password. Haz un telnet al modem y (10.0.0.138 subnet 255.255.0.0) pon cualquier nombre de usuario y el modem te contestara con algo como 'SpeedTouch (00-00-00-00-00-00)' antes de pedirte el password.

ESCRIBE ESTE NUMERO, DEBIDO A QUE NO HAY UNA FORMA SENCILLA DE RECUPERAR EL PASSWORD.

Entra a <http://security.sdsc.edu/self-help/alcatel/challenge.cgi> y sigue las instrucciones que se muestran en pantalla

Te van a dar un numero de respuesta ANOTALO TAMBIEN ESTE ES MUY IMPORTANTE.

Paso 2 - Activa las funciones PRO

Entra al modem usando telnet. Puedes entrar con cualquier usuario y password (si no lo haz cambiado) luego haz lo siguiente:

```
=> td
=> prompt
```

```
=====DISCLAIMER=====
Access to expert mode is intended for qualified personnel
only. Press ENTER to return to user mode.
=====END=OF=DISCLAIMER=====
```

SpeedTouch (00-00-00-00-00-00)'
password: el numero que te contestaron en la pagina de internet

Switched to 'Trace & Debug' prompt.

Return to Normal mode by typing <NORMAL>

>

Ya estas en el modo EXPERTO. Hay muchos comandos muy interesantes por aca.

El siguiente paso es convertir el modem en pro:

```
> rip
> drv_read 2 1 b
The Data in hex is : 8704
```

Anota este numero, lo necesitaras para regresarlo a la normalidad!!!!

Ahora toma el ultimo numero y cambialo a 6, ya que el 6 es el valor en hexadecimal que lo convierte en pro. Recuerda el ultimo numero siempre se convierte en 6.

```
rip> drv_write 2 1 b 8706
```

Reinicia el modem

```
rip>exit
>system
system> reboot
```

YA ES UN MODEM PRO!!!!!!

Nota: para regresarlo a la normalidad repite el procedimiento y en el paso de escribir cambia el:

```
rip> drv_write 2 1 b 8706
por
rip> drv_write 2 1 b 8704
```

Paso 3- Configura tu PC

Usa la siguiente configuracion en tu maquina

IP Address 10.0.0.x donde x no sea igual a 138 o mayor a 255 (creo que Es obvio por que).

```
Netmask 255.255.255.0
Default Gateway 10.0.0.138
Primary DNS normalmente 200.33.146.193 en el DF
Secondary DNS normalmente 200.33.146.201 en el DF
```

Paso 4 - Configura tu modem para PPP

Conectate a tu modem por la interface web a <http://10.0.0.138>. Haz click en System Setup y dale donde dice restore default factory settings y dale en Save All.

Vete a PPP y luego a configure en la primera entrada y elimina la segunda que dice PPP.

Configura la primera con los siguientes datos

```
Authentication
USa tu nombre de usuario del ADSL
Password Tu password
Routing
Connection Sharing Everybody
Destination networks All networks
Specific network dejalo vacio
NAT-PAT Enabled
Primary DNS DNS primario
Secondary DNS DNS secundario
Opciones
Local IP none
Remote IP none
Mode Dial-On
Idle time limit Vacio
LCP Echo Enabled
PAP Disabled
ACCOMP Enabled
```

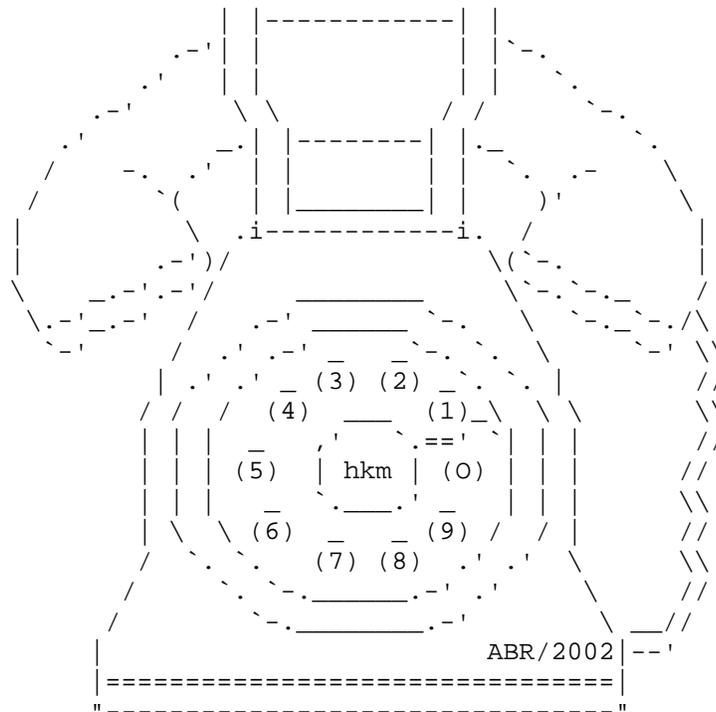
Dale en Apply y guarda los cambios . Teoricamente si haces click en Dial on y luego en dial ya

tendrias PPP en el modem, pero yo en lo personal no he logrado hacerlo, si alguien lo logra por favor mandeme un mail, El proximo numero estare escribiendo mas información de lo que vaya encontrando en el menu avanzado de configuracion del MODEM.

Normalmente estoy en irc.netshock.st los espero ahi si quieres platicar más sobre esto o sobre cualquier tema ;).

Diente
diente6@hotmail.com





1234567890123456789012345678901234567890123456789012345678901234567890

Bienvenido al archivo colectivo de los numeros escondidos de Telefonos de Mexico (TELMEX). El proposito de este documento es en su totalidad informativo, ningun colaborador / editor / autor asume responsabilidad alguna sobre lo que el lector pueda o lleve a cabo gracias a los datos aqui presentados.

La manera de funcionar de este llamado: "archivo colectivo" es trivial lo unico que tienes que hacer es checar, agregar o eliminar datos para formar un archivo que siempre este al corriente. Pondras tu nombre con los demas colaboradores y no borraras los que ya esten. Tambien puedes dejar un mensaje o alguna nota al final del mismo.

Estos son los numeros:

#001# = Linea (pero no puedes marcar) luego un tiempo y ocup...
 *080# = Te dice tu numero telefonico
 *12345678 = Terminal Uninet
 15?????# = Tonos diferentes y luego ocupado
 16?????# = Tonos diferentes y luego ocupado
 *20#????? = Buzon (? = clave de acceso de voz, numero)
 *21# = Su solicitud no ha sido registrada favor de repetir ...
 21?????# = Activar "Sigueme" (? = numero de telefono)
 #21# = Su solicitud ha sido registrada. Gracias.
 *24# = Su solicitud no ha sido registrada favor de repetir ...
 24????# = Su solicitud no ha sido registrada favor de repetir ...
 *31# = Ocupado
 #33*?????# = Ocupado
 33?????# = Su solicitud no ha sido registrada favor de repetir ...
 #34*?????# = Ocupado
 34?????# = Su solicitud no ha sido registrada favor de repetir ...
 #37# = Ocupado

#37*???...# = Ocupado
*39# = No contesta nada
43 = Activar "Llamada en espera"
#43# = Desactivar "Llamada en espera"
47???...# = Ocupado
#47*???...# = Ocupado
48???...# = Ocupado
#48*???...# = Ocupado
51???...# = Lo sentimos, el numero que usted marco no existe fav...
#51*???# = Su solicitud no ha sido registrada favor de repetir ...
53???...# = Su solicitud no ha sido registrada favor de repetir ...
#53# = Su solicitud no ha sido registrada favor de repetir ...
55?????# = Su solicitud no ha sido registrada favor de repetir ...
#55*?????# = Su solicitud no ha sido registrada favor de repetir ...
56?????# = Su solicitud no ha sido registrada favor de repetir ...
#56*12345# = Su solicitud ha sido registrada. Gracias
#56*?????# = Su solicitud no ha sido registrada favor de repetir ...
57???????# = Su solicitud no ha sido registrada favor de repetir ...
#57*???????# = Su solicitud no ha sido registrada favor de repetir ...
61???...# = Su solicitud no ha sido registrada favor de repetir ...
#61# = Su solicitud ha sido registrada. Gracias.
#62# = Su solicitud no ha sido registrada favor de repetir ...
63???# = Su solicitud no ha sido registrada favor de repetir ...
#63# = Su solicitud ha sido registrada. Gracias.
#66# = Su solicitud no ha sido registrada favor de repetir ...
#67# = Su solicitud ha sido registrada. Gracias.
68???# = Su solicitud no ha sido registrada favor de repetir ...
#69# = Su solicitud ha sido registrada. Gracias.
8477 = Servicio NOTICIAS
#99*?????# = Ocupado
97???...# = Estimado cliente su llamada no puede ser contestada...

Otros números:

01-800 123 2020 = Atencion a clientes (TELMEX)
01-800 123 4567 = LADA por cobrar a EEUU
01-800 123 3456 = Prodigy Internet de Telmex
01-800 123 2222 = Prodigy Internet de Telmex

Ya puedes ver mas números 800 en la siguiente dirección:
<http://www.telmex.com/internos/lada800/>

#COLABORADORES#####
#eagle4, hkm...

#####

#ULTIMA#REVISION#####
Jueves 12 de Abril del 2002 por hkm - hkm@hakim.ws #
#####

#MENSAJE#####
#Espero que alguien quiera colaborar, es en realidad un gran proyecto#
#Si tienen alguna duda, pueden mandarme un mail a: hkm@hakim.ws #
#####



Seminario de Programación
XROLEX

SAMSUNG SCH-A105 (WAP) (DUAL)

1. Prenda el aparato.

2. Inicie la programación tecleando **4 7 □ 8 6 9 # 0 8 # 9** , la pantalla mostrara la leyenda NAM Program 1 General, 2 Setup NAM 1, presione **21**, oprima **OK** para avanzar.

3. Introduzca uno a uno los siguientes parámetros:

Phone #	10 DIGITOS DE NUM.	OK	
Mobile ID	10 DIGITOS DE NUM.	OK	PRESIONAR 2
FM Home Side	01525	OK	
FM 1 st CH	333	OK	
FM Acq SID1	2	OK	
Acq SID2	0	OK	
FM Lock SID1	2000	OK	
Lock SID2	0	OK	
Auto Reg	Yes	OK	
FM Pref	A only		OK
FM ACCOLC	2	OK	PRESIONAR 3
INSI_MCC	000	OK	
INSI_MNC	00	OK	
CDMA Pref	A only		OK
ACCOLC	2	OK	
CDMA Primary Ch A	283	OK	
CDMA Primary Ch B	384	OK	
CDMA Second Ch A	691	OK	
CDMA Second Ch B	777	OK	
CD ACQ SID 1	2	OK	
CD ACQSID 2	0	OK	
CD LOCK SID 1	2000	OK	
CD LOCK SID 2	0	OK	
CDMA Home SID	YES	OK	
CDMA F SID	YES	OK	
CDMA F NID	YES	OK	
SID # 1	01525	OK	
NID # 1	0	OK	
SID # 2	0	OK	
NID # 2	65535	OK	
SID # 3	0	OK	
NID # 3	65535	OK	
SID # 4	0	OK	
NID # 4	65535	OK	

4. Para salir de la programación oprima **END**.

5. Verifique el numero programado presionando **MENU 42**.

6. Seleccione el sistema de operación tecleando **MENU 0**, seguido de su código de candado 0000, posteriormente presione **9**, y seleccione con **□** el sistema **A Only**, grabe con **OK**.

PROGRAMACIÓN IP SAMSUNG SCH-A 105 (WAP)

ACCESO A INTERNET

1. Teclar **MENU 7**
2. Presionar y sostener la tecla de **#** hasta que aparezca **CODIGO DE BLOQUEO**.
3. Teclar el código **0000** y aparecerá **NAVEGADOR**.
4. Seleccionar **GATEWAY 1** oprimiendo **1**
5. Si aparecen la direcciones presione **END** y listo, si no, aparecerán dos opciones **A** y **B**.
6. Seleccionar la opción **A** presionando **OK**, e ingresar la dirección **196.018.091.201**
7. Ingresar la dirección **196.018.091.202** y presionar **OK**.
8. Para salir presionar **END**.

DIRECCIÓN IP PRIMARIA (1) 196.018.091.201
DIRECCIÓN IP SECUNDARIA (2) 196.018.091.202

SAMSUNG SCH-M105 (MP3) (Rápida)

1. Prenda el aparato.

1. Inicie la programación tecleando **MENU 40** seguido de **000000**, la pantalla mostrara la leyenda NAM Program 1 Setup NAM 1, 2 Setup NAM 2 presione **1**, oprima **OK** para avanzar.

2. Introduzca uno a uno los siguientes parámetros:

Phone Number #	10	DIGITOS DE NUMERO	OK
Directory #	10	DIGITOS DE NUMERO	OK
Activar PRL	NO		OK
Dgtl HomeSID	01525		OK
Más programación	NO		OK

4. Para salir de la programación se presiona **END**.

4. El teléfono se reinicializa y vuelva a las condiciones iniciales.

5. Verifique el numero programado presionando **MENU 44**.

3. Seleccione el sistema de operación tecleando **MENU 0**, seguido de su código de candado 0000, posteriormente presione **9**, y seleccione con el sistema **A Pref**, grabe con **OK**.

SAMSUNG SCH-210/SCH- 410/SCH-411/SCH-811/SCH-620/SCH620i (DUALES)

• **OBTENCION DE LA SERIE:**

SE ENCUENTRA EN UNA ETIQUETA EN EL RADIO YA EN DECIMAL Y EMPIEZA CON 176 (PARA EL SCH-410 EL ESN EMPIEZA CON 241).

• **PARA ENTRAR A PROGRAMACION:**

ENCENDER, TECLEAR **47*869#08#9** APARECE NAM PROGRAM 1 GENERAL, 2 SETUP NAM1 , PRESIONE **21** (PARA NAM 1), AL INTRODUCIR INFORMACION OPRIMA **OK** PARA AVANZAR

SE RECOMIENDA QUE LOS PARAMETRO SE DEJEN TAL COMO ESTAN PROGRAMADOS Y SOLO SE MODIFIQUE EL NUMERO, EL FM HOME SID Y EL SID #1

• **INTRODUCIR UNO A UNO LOS SIGUIENTES PARAMETROS:**

<u>PHONE #</u>	10 DIGITOS DE NUM. TEL. OK	
MOBILE ID	10 DIGITOS DE NUM. TEL. OK	PRESIONE
2		
<u>FM HOME SID</u>	01525	OK
FM 1" CH	333	OK
FM ACQ SID1	2	OK
ACQ SID2	0	OK
FM LOCK SID1	2000	OK
LOCK SID2	0	OK
AUTO REG	YES	OK
FM PREF	A PREF	OK
FM ACCOLC	2	OK PRESIONE 3
AVANZAR CON OK (15 VECES) HASTA <u>SID #1</u>	01525	OK

AVANZAR CON OK HASTA **SETUP NAM1**

• **PARA SALIR DE PROGRAMACION:**

OPRIMA **END**

• **PARA PONER EN SISTEMA:**

PARA EL SCH-210 (PRESIONAR **MENU 0**, SEGUIDO DE CANDADO **0000**, ENSEGUIDA **9** Y CON FLECA HACIA ABAJO SELECCIONAR **A PREF** GRABAR CON OK).

PARA EL SCH-410 (PRESIONAR **MENU 0**, SEGUIDO DE CANDADO **0000**, ENSEGUIDA **92** Y CON FLECA HACIA ABAJO SELECCIONAR **A SOLO** GRABAR CON OK).

• **PARA VERIFICAR EL NUMERO DE TELEFONO:**

PARA EL SCH-210 (PRESIONE **MENU 42**).

PARA EL SCH-410/ SCH-411/SCH-811/SCH-620 (PRESIONE **MENU 22**).

PROGRAMACIÓN IP SAMSUNG SCH 620-I (WAP)

ACCESO A INTERNET

9. Teclear **MENU 6**.

10. Presionar y sostener la tecla de **#** hasta que aparezca **CODIGO DE BLOQUEO**.

11. Teclear el código **0000** y aparecerá **NAVEGADOR**.

12. Seleccionar **GATEWAY 1** oprimiendo **1**.

13. Si aparecen las direcciones programadas presione **END** y listo, si no, aparecerán dos opciones **A** y **B**.

14. Seleccionar la opción **A** presionando **OK**, e ingresar la dirección **196.018.091.201**

15. Ingresar la dirección **196.018.091.202** y presionar **OK**.

16. Para salir presionar **END**.

DIRECCIÓN IP PRIMARIA (1) 196.018.091.201
DIRECCIÓN IP SECUNDARIA (2) 196.018.091.202

PARA PROGRAMAR EL 2do NAM Y EN ALGUNOS MODELOS EL 3er Y 4to NAM. AL INGRESAR A PROGRAMACION CON **47*869#08#9**, PRESIONE **31** PARA **NAM 2** Y CUANDO APLIQUE **41** PARA **NAM 3** O **51** PARA **NAM 4**, POSTERIORMENTE SIGA CON LA MISMA SECUENCIA DE LA PROGRAMACION MOSTRADA ARRIBA.

PARA SELECCIONAR NAM: PRESIONE **MENU 0**, INGRESE CODIGO DE SEGURIDAD (0000 DE FABRICA) AVANZAR CON **#** HASTA **MODO NAM** Y PRESIONE **OK** SELECCIONE **MANUAL** Y PRESIONE **OK** , CON **#** ELIJA NAM A USAR Y PRESIONE **OK**.

SAMSUNG SH-800 (ANALOGICO)

• **OBTENCION DE LA SERIE:**

SE ENCUENTRA EN UNA ETIQUETA EN EL RADIO YA EN DECIMAL Y EMPIEZA CON 176

• **PARA ENTRAR A PROGRAMACION:**

ENCENDER, TECLEAR **47*869#08#9** ENTRA AUTOMATICAMENTE EN EL MODO DE PROGRAMACION.

• **INTRODUCIR UNO A UNO LOS SIGUIENTES PARAMETROS:**

(V)	SIDH	01525	AVANZAR CON TECLA LATERAL PARA ABAJO
	LOCAL	1	V
	MMARK	1	V
	TELNO	10	DIGITOS DE NUMERO V
	SCM	10	V
	IPCH	333	V
	ACCOL	02	V
	PS	1	V
	GIM	00	V
	LOCK	000	V
	DUAL	0 (UN NAM) ; 1 (DOS NAM'S)	V

SI SELECCIONA 2 NAM'S APARECE OTRA SECUENCIA IDENTICA A LA ANTERIOR, PERO PARA EL NAM 2.

• **PARA SALIR DE PROGRAMACION:**

OPRIMA **STO.**

• **PARA PONER EN SISTEMA:**

PRESIONAR **FCN 0** SEGUIDO DE 3 DIGITOS DE CANDADO (000) , CON TECLAS LATERALES SELECCIONAR **A ONLY** Y PRESIONAR **STO.**

• **PARA VERIFICAR EL NUMERO DE TELEFONO:**

PRESIONAR **RCL #.**

SHINTOM 8700/8800 (ANALOGICOS)

• **OBTENCION DE LA SERIE:**

SE ENCUENTRA EN UNA ETIQUETA EN EL RADIO YA EN DECIMAL Y EMPIEZA CON 174

• **PARA ENTRAR A PROGRAMACION:**

FCN 5 PARA BLOQUEAR EL TELEFONO, **FUNC # 626 # FUNC**, APARECE NUMERO DE MODELO Y VERSION DE SOFTWARE CONFIRMANDO QUE SE ENTRO A PROGRAMACION.

• **PARA GRABAR LOS DATOS:**

1 AREA CODE	524 SEND
2 TELEFONO	ULTIMOS 7 DIGITOS DEL TELEFONO SEND
3 SIDH	01525 SEND
4 ACCESS OVERLOAD	02 SEND
5 GIM	00 SEND
6 LOCAL USE	1 SEND
7 MIN OPT	1 SEND
8 CANDADO	123 SEND
9 CANDADO AUTOMATICO	0 SEND
10 APARECE LA CLAVE DEL PASO 8	

• **PARA SALIR DE PROGRAMACION:**

END FCN END AL SALIR DE PROGRAMACION EL EQUIPO ESTARA BLOQUEADO, TECLEAR LA CLAVE DEL PASO 8 PARA DESBLOQUEAR.

• **PARA PONER EN SISTEMA:**

FNC 7

• **PARA VERIFICAR EL NUMERO DE TELEFONO:**

NO ES POSIBLE EN MODO DE USUARIO

SIEMENS S850 (ANALOGICO)

• **OBTENCION DE LA SERIE:**

DIRECTAMENTE SE ENCUENTRA EN LA ETIQUETA POSTERIOR E INICIA CON **208**
TAMBIEN VIENE EN HEXADECIMAL E INICIA CON **D0**

• **PARA ENTRAR A PROGRAMACION:**

ENCENDER, TECLEAR **OK OK *697601*** AVANZAR CON FLECHA HACIA ARRIBA

• **INTRODUCIR UNO A UNO LOS SIGUIENTES PARAMETROS, PRESIONANDO # PARA GRABAR Y FLECHA HACIA ARRIBA PARA AVANZAR.**

SIDH	01525	# / \
SCM	10	# / \
MIN	10 DIGITOS DE NUM. TEL.	# / \
IDCCA	0333	# / \
IDCCB	0334	# / \
IPCH	0333	# / \
ACCOLC	02	# / \
GIM	00	# / \
INV-SID1	00000	# / \ .
.		
INV-SID8	00000	# / \
OPTION LC	0	# / \
OPTION EX	0	# / \
OPTION PS	1	# / \
OPTION NSC	0	# / \
OPTION HA	0	# / \
OPTON HF	0	# / \
OPTION F1	0	# / \ .
.		
OPTION F7	0	# / \
COLCK CODE	1234	# / \
SECUCODE	5678	# / \
BANNER		

• **PARA SALIR DE PROGRAMACION:**

OPRIMA **OK END END**

• **PARA PONER EN SISTEMA:**

PRESIONAR **MENU 52**, Y CON **MENU SELECCIONAR SYSTEM PREFER A** SALIR CON **END**

• **PARA VERIFICAR EL NUMERO DE TELEFONO:**

PRESIONE **MENU 51**

SONY CM-RX100

- **OBTENCION DE LA SERIE:**

AL NUMERO DE LA ETIQUETA QUE ESTA EN LA PARTE POSTERIOR DESPUES DE QUE SE RETIRO LA BATERIA, SE ANTEPONE 1540 Y ES EL NUMERO EN DECIMAL.

- **PARA ENTRAR A PROGRAMACION:**

ENCENDER, TECLEAR #6269781 APARECE SYSTEM ID QUE TIENE PROGRAMADO

- **PARA GRABAR LOS DATOS:**

01525 #

ULTIMOS SIETE DIGITOS DEL NUMERO #

PRIMEROS 3 DIGITOS DEL NUMERO#

MUESTRA EL NUMERO COMPLETO NO TECLEAR MAS QUE #

CANDADO 1234#

1 #

1 #

1110 #

0333 #

0333 #

0334 #

02 #

1 #

00 #

0 #

- **PARA SALIR DE PROGRAMACION:**

END

- **PARA PONER EN SISTEMA:**

PRESIONAR **SELECT** Y GIRAR HASTA **FUNC 61**, NUEVAMENTE **SELECT** Y **1** PARA SOLO A, SE BORRA SOLO DESPUES DE UN MOMENTO.

- **PARA VERIFICAR EL NUMERO DE TELEFONO:**

RCL #

SONY CM-R111

• **OBTENCION DE LA SERIE:**

AL NUMERO DE LA ETIQUETA QUE ESTA EN LA PARTE POSTERIOR DESPUES DE QUE SE RETIRO LA BATERIA, SE ANTEPONE 1540 Y ES EL NUMERO EN DECIMAL. PARA ALGUNOS MAS ANTIGUOS SE CONVIERTE COMO SI FUERA DE PANASONIC: UN NUMERO DEL TIPO N-OPQRST, A PARTIR DE ESTE NUMERO SE OBTIENE LA SERIE EN DECIMAL DE LA SIGUIENTE FORMA:

EL NUMERO N SE MULTIPLICA POR 262144 Y AL RESULTAD SE LE SUMA EL OPQRST; POR EJEMPLO: SI EL NUMERO ES 4-042540, LA OPERACIÓN SERIA:

$4 \times 262144 = 1048576 + 042540 = 1091116$ Y LA SERIE ES 13601091116

• **PARA ENTRAR A PROGRAMACION:**

ENCENDER, TECLEAR #6269781 SE ESCUCHA UN TONO DOBLE COMO CONFIRMACION

• **PARA GRABAR LOS DATOS:**

#0101525# Y SE ESCUCHA UN DOBLE "BEEP"

#02729XXXX# Y SE ESCUCHA UN DOBLE "BEEP"

#04524# Y SE ESCUCHA UN DOBLE "BEEP"

#051# Y SE ESCUCHA UN DOBLE "BEEP"

#061# Y SE ESCUCHA UN DOBLE "BEEP"

#071010# Y SE ESCUCHA UN DOBLE "BEEP"

#080333# Y SE ESCUCHA UN DOBLE "BEEP"

#090333# Y SE ESCUCHA UN DOBLE "BEEP"

#100334# Y SE ESCUCHA UN DOBLE "BEEP"

#1102# Y SE ESCUCHA UN DOBLE "BEEP"

#121# Y SE ESCUCHA UN DOBLE "BEEP"

#1300# Y SE ESCUCHA UN DOBLE "BEEP"

#230# Y SE ESCUCHA UN DOBLE "BEEP"

• **PARA SALIR DE PROGRAMACION:**

END

• **PARA PONER EN SISTEMA:**

RCL *5

• **PARA VERIFICAR EL NUMERO DE TELEFONO:**

NO ES POSIBLE POR LA FALTA DE PANTALLA

SONY 1300 (DUAL)

OBTENCION DE LA SERIE:

TRAE UNA ETIQUETA EN LA PARTE POSTERIOR CON LA SERIE EN DECIMAL E INICIA CON **211**

• **PARA ENTRAR A PROGRAMACION:**

INTRODUZCA LA SIGUIENTE SECUENCIA, **111111** , EN SEGUIDA PRESIONAR EL DIAL 2 VECES, DIGITE **000000**.

INTRIDUCIR LOS DATOS UNO A UNO Y PRESIONAR EL DIAL PARA GRABAR Y AVANZAR

• **PARA GRABAR LOS DATOS:**

AL INICIO APARECE EL ESN		PRESIONAR DIAL OK
PHONE#	10 DIGITOS DE NUMERO	PRESIONAR DIAL OK
HOME SIDH	01525	PRESIONAR DIAL OK
NAME	-----	PRESIONAR DIAL OK
BASIC NAM 1		PRESIONAR DIAL OPTIONS
OPTIONS	SELECCIONAR EXIT	PRESIONAR DIAL EXIT

• **PARA SALIR DE PROGRAMACION:**

EN OPTIONS SELECCIONAR EXIT Y PRESIONAR DIAL

• **PARA PONER EN SISTEMA:**

PRESIONAR DIAL EN **FEATURES** Y EN SEGUIDA **75**, SELECCIONAR HOME SIDE GIRANDO EL DIAL Y ACEPTAR PRESIONANDO EL DIAL

• **PARA VERIFICAR EL NUMERO DE TELEFONO:**

PRESIONAR DIAL EN **FEATURES** Y EN SEGUIDA **31**

TECHNOPHONE 205/205^a (ANALOGICOS)

• **OBTENCION DE LA SERIE:**

EN LA ETIQUETA DE LA PARTE POSTERIOR ESTA EN HEXADECIMAL EMPIEZA CON A2, HAY UNO EN DECIMAL QUE EMPIEZA CON 162, PERO NO ES CORRECTO, SIEMPRE SE DEBE OBTENER A TRAVEZ DEL QUE VIENE EN HEXADECIMAL

• **PARA ENTRAR A PROGRAMACION:**

000000## 953739# MEM 99 MEM MEM APAGAR Y ENCENDER, APARECE NO OF NAMS

• **PARA GRABAR LOS DATOS:**

1 F

F

01525 F

F

524 F

DESPLIEGA EL VALOR ANTERIOR F

ULTIMOS 7 DEL NUMERO DE TELEFONO F

DESPLIEGA EL VALOR ANTERIOR F

02 F

1 F

F

011 F

911 F

0 F

WICH NAM?

• **PARA SALIR DE PROGRAMACION:**

* F

• **PARA PONER EN SISTEMA:**

F3 CON F HASTA PREF END

• **PARA VERIFICAR EL NUMERO DE TELEFONO:**

F2, END

TECHNOPHONE 400/405/415 (ANALOGICOS)

• **OBTENCION DE LA SERIE:**

DIRECTO EN ETIQUETA EN LA PARTE POSTERIOR DEL TELEFONO, COMIENZA CON 156 Y ESTA EN DECIMAL.

• **PARA ENTRAR A PROGRAMACION:**

ENCENDER *3001 # 12345 STO 00

• **PARA GRABAR LOS DATOS:**

PARA EL PC415 *911#911#2*12345 STO 01 STO

PARA EL PC400 PC405 *911#911#2*1234 STO 01 STO

TELEFONO DE 10 DIGITOS STO 02 STO

01525*1*1*333*02*00 STO 03 STO

• **PARA SALIR DE PROGRAMACION:**

APAGAR Y ENCENDER

• **PARA PONER EN SISTEMA:**

PARA EL 400 **F1** CON FLECHAS HASTA A **STO**

PARA EL 405 **F1** CON FLECHAS HASTA A **ONLY STO**

PARA EL 415 **MENU 1** CON FLECHAS HASTA A **STO**

• **PARA VERIFICAR EL NUMERO DE TELEFONO:**

PARA EL 400 **F7 CLR**

PARA EL 405 **F7 CLR**

PARA EL 415 **MENU 7**

TECHNOPHONE PC515 (ANALOGICO)

• **OBTENCION DE LA SERIE:**

DIRECTO DE LA ETIQUETA EMPIEZA CON 156

• **PARA ENTRAR A PROGRAMACION:**

*3001#12345 STO 00 APARECE STORE NOT DONE O GRABACION NO HECHA, ELLO INDICA QUE SE ENTRO A PROGRAMACION, SI APARECE NOT ALLOWED O NO PERMITIDO NO SE ENTRO Y SE DEBE INTENTAR NUEVAMENTE.

• **PARA GRABAR LOS DATOS:**

*911#2 STO 01 STO
NUMERO DE TELEFONO DIEZ DIGITOS STO 02 STO
01525*1*1*333*02*00#95*52*91 STO 03 STO

• **PARA SALIR DE PROGRAMACION:**

APAGAR Y ENCENDER, SI APARECE NAM ERROR, SE DEBE PROGRAMAR NUEVAMENTE CUIDANDO DE NO COMETER ERRORES AL TECLEAR LOS VALORES.

• **PARA PONER EN SISTEMA:**

FCN, FCN, 3 CON FCN HASTA PREF Y CLR

• **PARA VERIFICAR EL NUMERO DE TELEFONO:**

FCN 1, CLR

TECHNOPHONE 900/905A/905MKII/985A/995 (ANALOGICOS)

• **OBTENCION DE LA SERIE:**

TECLEAR **MU 01** Y APARECE EN PANTALLA EN HEXADECIMAL A2...

• **PARA ENTRAR A PROGRAMACION:**

ENCENDER, TECLEAR **#00000##953739# STO 99 STO STO**, APAGAR Y ENCENDER, APARECE WHICH NAM, TECLEAR EL NUMERO DE NAM QUE SE VA A PROGRAMAR, NORMALMENTE UNO Y **STO**, APARECE EL SIDH QUE TIENE PROGRAMADO.

• **PARA GRABAR LOS DATOS:**

MODELOS 905 A/ 905MKII/985 A/ 995 MODELOS 900/900BC Y 901

01525 *

TEL 10 DIGITOS *

02 *

1 *

333 *

STO

SAVE NAM?

01525 STO

TEL 10 DIGITOS STO

00 STO SI APARECE SAVE NAM DAR STO

STO

STO

STO

911 STO

011 STO

02 STO

1 STO

0333 STO

0333 STO

0334 STO CON STO HASTA QUE SALGA:

SAVE NAM?

• **PARA SALIR DE PROGRAMACION:**

SEND Y LUEGO **END END** APAGAR Y ENCENDER

• **PARA PONER EN SISTEMA:**

MODELOS 905 A/ 905MKII/985 A/ 995 MODELOS 900/900BC Y 901

MU 21 CON **MU** HASTA **AB CLR**

MENU 5 CON **MENU** HASTA **PREF END**

• **PARA VERIFICAR EL NUMERO DE TELEFONO:**

MU 22

MENU MENU MENU, CLAVE CANDADO (0000)

1 MENU MENU END

TECHNOPHONE 915^a (ANALOGICO)

• **OBTENCION DE LA SERIE:**

CON MU 05 APARECE EN PANTALLA EN HEXADECIMAL A2...

• **PARA ENTRAR A PROGRAMACION:**

ENCENDER, TECLEAR #000000##953739# STO 29 STO STO, APAGAR Y ENCENDER
APARECE WHICH NAM?, DAR 1 ó 2 STO

• **PARA GRABAR LOS DATOS:**

01525 *

TELEFONO DIEZ DIGITOS *

02 *

00 *

1 *

333 *

CON * HASTA QUE APARECE WHICH NAM?

• **PARA SALIR DE PROGRAMACION:**

SEND, END. APAGAR Y ENCENDER

• **PARA PONER EN SISTEMA:**

MU 11 CON MU HASTA AB CLR

• **PARA VERIFICAR EL NUMERO DE TELEFONO:**

TOSHIBA TCP9600 (ANALOGICO)

• **OBTENCION DE LA SERIE:**

DIRECTAMENTE DE LA ETIQUETA DE LA PARTE DE ATRÁS QUE COMIENZA CON 138, SI LE FALTA LA ETIQUETA CUALQUIER OTRO NUMERO NO SIRVE PARA OBTENER LA SERIE.

• **PARA ENTRAR A PROGRAMACION:**

CLAVE FCN # 1 DONDE LA CLAVE PUEDE SER: LOS TRES ULTIMOS DIGITOS DEL NUMERO DE SERIE O DEL TELEFONO QUE TRAE PROGRAMADO, 123, 000, 111, DE NO FUNCIONAR ALGUNO DE ESTOS ACUDIR A SERVICIO TECNICO.

SI SE LOGRO ENTRAR A PROGRAMACION APARECE 01 TEL EN LA PARTE SUP DE LA PANTALLA Y EL NUMERO QUE TIENE GRABADO ABAJO.

• **PARA GRABAR LOS DATOS:**

01 TEL NO. 10 DIGITOS DEL TELEFONO M/ALPH
02 LOCK CODE TRES DIGITOS DE CANDADO M/ALPH
03 SIDH 01525 M/ALPH
04 OLC 02 M/ALPH
05 GIM 00 M/ALPH
06 LU 1 M/ALPH
07 MIN 1 M/ALPH
08 IPCH 0333 M/ALPH
09 PS 1 M/ALPH
10 SCM 1010 M/ALPH
11 FUNCTION 1 10110000 M/ALPH
12 FUNCTION 2 00000000 NO TECLEAR NADA, SALIR DE PROGRAMACION.

• **PARA SALIR DE PROGRAMACION:**

FCN SEND, APARECE NAM WRITING Y LUEGO CHECK ADJ. CON UN DATO X EN PANTALLA, **FCN CLR**.

• **PARA PONER EN SISTEMA:**

FNC 81 CON # HASTA PRF SYS R/ST END

• **PARA VERIFICAR EL NUMERO DE TELEFONO:**

R/ST #, CLR

UNIDEN 4600/4900/5600/6600 (ANALOGICO)

• **OBTENCION DE LA SERIE:**

TRAE UNA ETIQUETA EN LA PARTE POSTERIOR CON LOS ULTIMOS OCHO DIGITOS DE LA SERIE EN DECIMAL, ANTEPONER 172

• **PARA ENTRAR A PROGRAMACION:**

ENCENDER, PRESIONAR DE INMEDIATO # y * SIMULTANEAMENTE Y NO SOLTAR HASTA QUE EN LA PANTALLA QUEDEN SOLO TODOS LOS INDICADORES ROAM, NO SVC, IN USE & M; TECLEAR 32218591 (EN MENOS DE 7 SEGUNDOS). APARECE TEST MODE SELECT. PRESIONAR 2 Y APARECE NAM DAR 1, APARECE ITEM

• **PARA GRABAR LOS DATOS:**

0 01525 STO
1 1 STO
2 1 STO
3 TEL 10 DIGITOS STO
4 333 STO
5 02 STO
6 1 STO
7 00 STO
8 1234 (CANDADO) STO

• **PARA SALIR DE PROGRAMACION:**

SEND, END APAGAR Y ENCENDER

• **PARA PONER EN SISTEMA:**

MENU Y CON FLECHAS HASTA SYSTEM SELECT STO CON FLECHAS HASTA A ONLY STO CLR

• **PARA VERIFICAR EL NUMERO DE TELEFONO:**

MENU CON FLECHAS HASTA NAM SELECT STO STO CLR

UNIDEN 5500 (ANALOGICO)

• **OBTENCION DE LA SERIE:**

TRAE UNA ETIQUETA EN LA PARTE POSTERIOR CON LOS ULTIMOS OCHO DIGITOS DE LA SERIE EN DECIMAL, ANTEPONER 172

• **PARA ENTRAR A PROGRAMACION:**

APAGAR PRESIONAR Y MANTENER # Y *, SIN SOLTARLAS ENCENDER EL EQUIPO Y NO SOLTAR LAS TECLAS HASTA QUE LOS INDICADORES DE ROAM, NO SVC, IN USE Y M QUEDEN ENCENDIDOS; TECLEAR **32218591** APARECE EL VALOR DEL SIDH

• **PARA GRABAR LOS DATOS:**

0 01525 STO

1 1 STO

2 1 STO

3 TEL 10 DIGITOS STO

4 333 STO

5 02 STO

6 1 STO

7 00 STO

8 1234 (CANDADO) STO

• **PARA SALIR DE PROGRAMACION:**

SEND, END, APAGAR Y ENCENDER

• **PARA PONER EN SISTEMA:**

1 STO 88

• **PARA VERIFICAR EL NUMERO DE TELEFONO:**

RCL 99

UNIDEN 7500 (ANALOGICO)

- **OBTENCION DE LA SERIE:**

TRAE UNA ETIQUETA EN LA PARTE POSTERIOR CON LOS ULTIMOS OCHO DIGITOS DE LA SERIE EN DECIMAL, ANTEPONER 172

- **PARA ENTRAR A PROGRAMACION:**

ENCENDER, PRESIONAR DE INMEDIATO # y * SIMULTANEAMENTE Y NO SOLTAR HASTA QUE EN LA PANTALLA QUEDEN SOLO TODOS LOS INDICADORES ROAM, NO SVC, IN USE & M; TECLEAR 32218591 (EN MENOS DE 7 SEGUNDOS). APARECE TEST MODE SELECT. CON TECLAS DE FLECHAS HASTA NAM WRITE, PRESIONAR **STO** APARECE NAM NO PRESIONAR 1 APARECE PASO 0 CON EL SIDH QUE TIENE ACTUALMENTE.

- **PARA GRABAR LOS DATOS:**

01525 FLECHA HACIA ABAJO
1 FLECHA HACIA ABAJO
1 FLECHA HACIA ABAJO
10 DIGITOS DEL TEL FLECHA HACIA ABAJO
0333 FLECHA HACIA ABAJO
02 FLECHA HACIA ABAJO
1 FLECHA HACIA ABAJO
00 FLECHA HACIA ABAJO
CANDADO 1234 FLECHA HACIA ABAJO
1 FLECHA HACIA ABAJO

- **PARA SALIR DE PROGRAMACION:**

STO, END APAGAR Y ENCENDER.

- **PARA PONER EN SISTEMA:**

MENU 0 STO STO CON FLECHAS HASTA A ONLY **STO**

- **PARA VERIFICAR EL NUMERO DE TELEFONO:**

MENU 5 STO, STO

AUDIOVOX MVX425/MVX450/MVX480 (ANALOGICOS)

• **OBTENCION DE LA SERIE:**

ETIQUETA EN PARTE POSTERIOR EN DECIMAL QUE EMPIEZA CON **138 O 242**, CUALQUIER OTRO NUMERO NO SIRVE PARA OBTENER LA SERIE; SI NO TRAE LA ETIQUETA NO SE OBTENDRA DIRECTAMENTE.

• **PARA ENTRAR A PROGRAMACION:**

CLAVE FCN # 81 DONDE LA CLAVE PUEDE SER: (DE FABRICA 000) ; LOS TRES ULTIMOS DIGITOS DEL NUMERO DE SERIE O DEL TELEFONO QUE TRAE PROGRAMADO, 123, 111, DE NO FUNCIONAR ALGUNO DE ESTOS ACUDIR A SERVICIO TECNICO.

SI SE LOGRO ENTRAR A PROGRAMACION APARECE UN 01 EN LA PANTALLA Y LOS TRES PRIMEROS DIGITOS DEL NUMERO QUE TIENE GRABADO A UN LADO.

SOLO PROGRAMAR NUMERO (LOS 3 PRIMEROS PASOS), SIDH Y CLAVE DE CANDADO, LO DEMÁS DEJARLO COMO VENGA.

• **PARA GRABAR LOS DATOS:**

1 AREA	524	FLECHA PARA ABAJO
2 CIUDAD	727	FLECHA PARA ABAJO
3 NUMERO	XXXX	FLECHA PARA ABAJO
4 CLAVE CANDADO	123	FLECHA PARA ABAJO
5 SIDH	01525	FLECHA PARA ABAJO
6 ACCESS OVERLOAD 02		FLECHA PARA ABAJO
7 GIM	00	FLECHA PARA ABAJO
8 LOCAL USE	1	FLECHA PARA ABAJO
9 MIN OPT	1	FLECHA PARA ABAJO
10 INITIAL PAGING CH	333	FLECHA PARA ABAJO
11 PREF SYST	1	FLECHA PARA ABAJO
12 SCM	1010	FLECHA PARA ABAJO
13 OPTIONS	10100	FLECHA PARA ABAJO
14 NO IMPORTA LO QUE SALGA		
15		
16		

• **PARA SALIR DE PROGRAMACION:**

FUNC SEND APARECE UN DATO CUALQUIERA EN PANTALLA, **FCN CLR**

• **PARA PONER EN SISTEMA:**

FUNC 7 CON # HASTA A **SYS END**

• **PARA VERIFICAR EL NUMERO DE TELEFONO:**

FCN 0

SI ES REPROGRAMACION, EL EQUIPO SE PROGRAMA COMO SIGUE:
01525524XXXXXXXX FNC 8. (SIDH+NUMERO+FCN 8)

NOKIA 5120

- a) * # 639 # NUMERO TELEFONICO(524X-XX XX XX) OK 01525

PROGRAMACIÓN LARGA

- a) *3001 # 12345 #
- b) OPRIMIR 1 PARA SELECCIONAR NAM 1
- c) (oprimir selec) Introducir el HOME SID 01525
- d) (oprimir selec) Introducir Home SOC 12
- e) (oprimir selec) Introducir own number 52-4X-XX-XX-XX
Ir hasta Cange defaultls oprimir (oprimir selec)

- a. Ir hasta Secundari PaginCH (oprimir selec) Introducir 708
- b. Dedicated A cch (oprimir selec) Introducir 333
- c. Dedicated A cch Number (oprimir selec) Introducir 20
- d. Dedicated B cch (oprimir selec) Introducir 334
- e. Dedicated B cch Number (oprimir selec) Introducir 20
- f. Overload class (oprimir selec) Introducir 2
- g. Groupm ID (oprimir selec) Introducir 10 ò 0
- h. APAGAR Y PRENDER EL EQUIPO

PARA VERIFICAR NUMERO PROPIO **MENU 4 5 1**

ERICSSON 668 (Digital)

- 1) Se prende el equipo
- 2) Inicie la programación tecleando 923885 idespues la flecha hacia la derecha(o abajo)
- 3) Aparece elnumero de serie como prueba de que se entro a la programación
- 4) Introducir el numero telefonico (52-4X-XX-XX-XX)en el espacio correspondiente, asi como el HOME SID **01525**
- 5) SALIR DE LA PROGRAMACIÓN TECLEANDO SEND

**PROCEDIMIENTO PARA SACAR NUM. DE SERIE DE MOTOROLA (PLATINIUM 850,
TELETAC, MICROTAC)**

Para quitar funciones (RECETEO) de MOTOROLA STAR TAC :

FCN 00 ** 83 78 66 33 STO # 32 # y aparecerá entonces una ,
(coma) y un sonido
esperar hasta que ese sonido desaparezca y marcar entonces 01 # .

Para Sacar numero de SERIE de MOTOROLA STAR TAC :

FCN 00 ** 83 78 66 33 STO # 32 # y aparecerá entonces una ,
(coma) y un sonido
esperar hasta que ese sonido desaparezca y marcar entonces 38 # .
aparecera el numero de SERIE en extra-decimal.

DIAGRAMA DE FLUJO DE EMULADOR DE CARTMAN
Por Illan Ivanovich

Vamos a tratar de analizar la naturaleza de la emulación en el proyecto de cartman. Y para esto nos vamos a basar primeramente en el diagrama de flujo que tiene en su page. Espero que este doc sea de utilidad para todos los que se quieren iniciar en esto y que sea como una invitación para los que ya saben y que nos quieran seguir enseñando.

También aprovecho para invitarlos a investigar y a demostrar que también los mex tenemos huev.. en la cabeza para poder entender todo este show. Es un poco difícil encontrar gente que se dedique tanto, he visto los foros de España donde hay hasta 900 posts en un solo tema, yo sé que la economía mexicana no está como para dedicarse a un hobby como este pero insisto: Invito a todos los mexicanos entusiastas, hobbistas y profesionales a demostrar que también somos chingones.

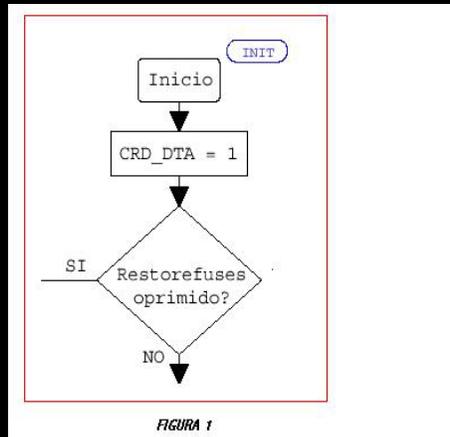
NOTA: Como se darán cuenta, mi análisis es un tanto rebuscado y tosco ya que también he ido aprendiendo poco a poco, posiblemente o seguramente me equivoqué en algunos puntos pero para cualquier duda o aclaración mándenme un mail: illan_ivanovich@yahoo.com

Como sugerencia deberán tener a la mano el diagrama de flujo del emu de Cartman para que vayan entendiéndolo mejor. Recuerde que este diagrama de flujo lo puede encontrar en la pagina de Cartman: cartman0.cjb.net en esta pagina también encontrarán el esquemático. Aclaremos que solo estamos analizando el diagrama de flujo de cartman y no intentamos explicar como construir una tarjeta de teléfono falsa, para el que piense que esto se trata de defraudar a alguien se está equivocando.

Este documento es solo con fines de investigación y el autor no se hace responsable del mal uso que se le pueda dar.

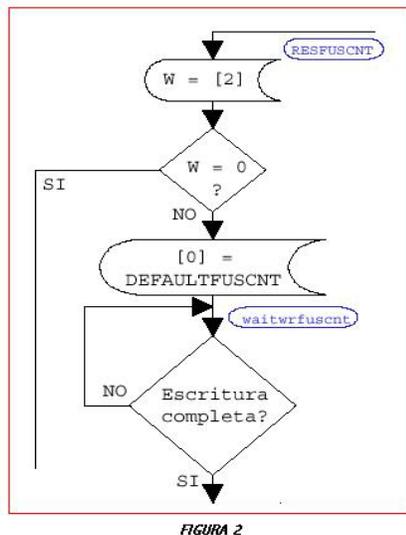
CARTMAN: Una vez mas estoy usando tu trabajo con fines de aprendizaje, espero no te moleste. También espero que puedas hacer las correcciones necesarias para sugerir el doc en algunas páginas que puedan estar interesadas en hospedarlo. Agradezco el interés que le has puesto al tema, ya que con eso nos ayudas a tener iniciativa en la investigación.
Gracias...
Bk

INICIEMOS



Etiqueta INIT es donde el programa comienza a hacer su show. Una de los puntos importantes es el de mantener el valor de CRD_DATA en 1. Posteriormente checamos el estado del microswitch de recarga de tarjeta, en caso de estar oprimido nos vamos a la rutina de recarga de tarjeta que es lo que explicaremos a continuación:

RESFUSCNT



Checamos el contenido en eeprom en la dirección 02 (Fig 2). Esta dirección de eeprom es utilizada para saber si se ha hecho una recarga recientemente, ya que en programa principal esta dirección se pone a ff de valor. Por lo tanto la dirección 2 de eeprom va a ser utilizada como un flag que nos va a indicar cuando ya se hizo una recarga.

Cuando es igual a cero vamos al final de la rutina de recarga y no se hace nada y cuando es diferente de cero significa que ya se usó y que ahora si se puede hacer la recarga (Fig 2).

Aquí, el programa cargará en la dirección cero de eeprom el valor de DEFAULTFUSCNT (Contador de fusibles), cabe aclarar que este es una constante que se definió en el principio del programa con el valor decimal de 5. EL FUSCNT se explicará al final del doc. NOTA: El defaultfuscnt no es mas que el crédito que ya se gastó. Cartman supone en

su programa que se han gastado 5 unidades cada vez que se recarga (Fig 2).

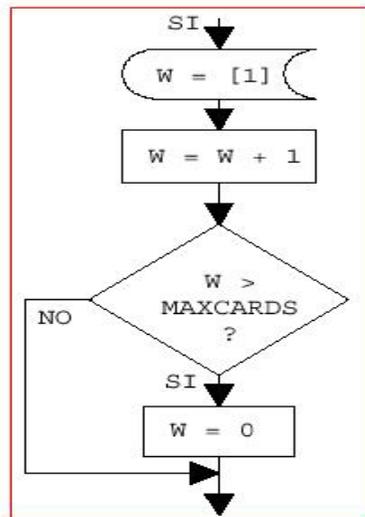


FIGURA 3

Checamos el contenido de la dirección 1 de eeprom (CRDCNT) este es el contador de tarjetas que se han utilizado y no debe pasar de 21 (Fig 3). Aquí aumentamos el valor de crdcnt en 1 y checamos si llegó al máximo de lo permitido. (Figura 3)

Si llegó al máximo de lo permitido hacemos w=0 y lo almacenamos en la dir 1 de eeprom que es donde se guarda el crdcnt (Resetaeamos el contador de tarjetas Fig 4).

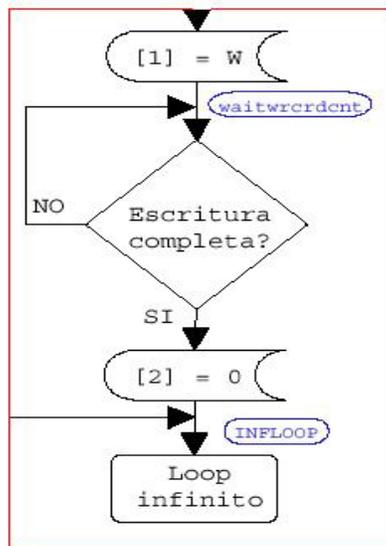


FIGURA 4

Si no ha llegado al máximo entonces nos vamos al final del programa y almacenamos en la dirección 2 de eeprom el valor cero y terminamos la rutina de recarga (Fig 4).

Como conclusión podemos mencionar que en esta rutina de recarga se manipularon tres registros o direcciones de eeprom las cuales son:
 Dirección 00h es donde se almacena el contador de fusibles
 Dirección 01h es donde almacenamos el valor de las tarjetas gastadas
 Dirección 02h es un flag auxiliar que nos permite realizar una recarga cada vez que sea necesario y no una tras otra.

RESTOREFUSES SIN OPRIMIR.

Aquí empieza la parte del programa cuando no se ha oprimido el microswitch. Aclaremos que en este punto no se han habilitado las interrupciones por lo que en caso de que la cabina nos mande un reset, el emulador no lo reconocería.

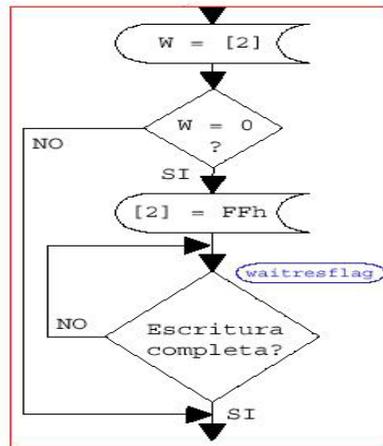


FIGURA 5

Checamos el valor de la dirección 02h de eeprom (Fig 5). Recuerde que en caso de que sea cero significa que se acaba de ejecutar una recarga y por lo tanto le cargamos un valor diferente de cero (en este caso el valor FFh) para que a partir de este momento se tenga la posibilidad de recarga.

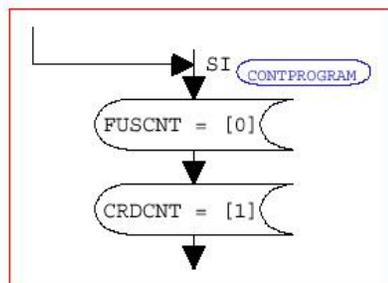


FIGURA 6

Asignamos al registro FUSCNT lo contenido en la dirección 00h de eeprom (Fig 6). Aquí debemos recordar que este registro guarda el valor 5 cuando hacemos la recarga por medio de DEFAULTFUSCNT. Por que se usa este valor???? Lo veremos en la rutina de interrupción no os desesperéis mis muchachitos..

Se asigna a CRDCNT lo contenido en la dirección 01h de eeprom (Fig 6), en este momento CRDCNT contiene el valor de las tarjetas que se han usado y

que van de 1 a 21. La dirección 01h de eeprom es modificada cada vez que se hace una recarga.

Aquí hay algo importante: Si se dan cuenta, en la rutina de recarga de tarjeta tenemos que almacenar cambios en la eeprom del PIC. Esto lo hace de una manera lenta. La cabina se puede valer del envío de voltajes de VCC para alimentar a la tarjeta muy cortos, por lo cual podría afectar nuestra recarga.

Aclaremos que para efectuar la recarga debemos introducir la tarjeta a la cabina con el switch activado y retirarla, esto no debe llevar mas de algunos milisegundos. Pero en caso de que no se pudiera hacer la recarga en la cabina podríamos optar por una fuente externa, pero "esa... es otra historia.."

Ahora viendo la rutina de inicio sin el restorefuses oprimido encontramos que la mayoría de los cambios que se realizarán van a ser solamente en la RAM del PIC, solamente observaremos algunos cambios en eeprom que serán la dirección 02h y la dirección 0.

Ahora viene algo bueno: El valor de las tarjetas que se han usado se multiplica por doce 12. A chis porque?? (Fig 7)

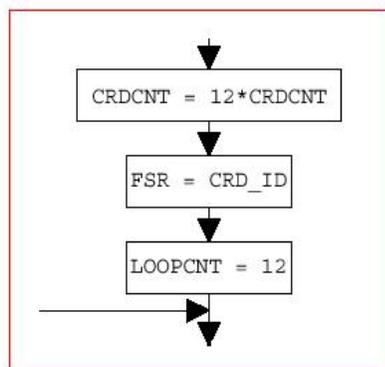


FIGURA 7

Por que cada tarjeta que se usa contiene 12 bytes de header. Aquí vamos a usar el CRDCNT como contador de headers y dejará de usarse (Por este momento) como contador de tarjetas usadas. Ejemplo: Si ya se usaron 3 tarjetas entonces CRDCNT=3 y posteriormente CRDCNT=36 el cual va a ser usado por FSR para posicionarse en el primer dato del tercer HEADER. (Fig 7)

Si alguien no sabe que es el header que lastima.. No, el header no es mas que los primeros 12 bytes de datos de la tarjeta donde se encuentra el saldo, el número de serie y el checksum.

Asignamos el valor de CRD_ID a FSR, les recomiendo que se chequen un poco acerca de direccionamiento indirecto a travez de FSR e INDF. Posteriormente tenemos el LOOPCNT=12, este registro especial nos va a servir para hacer el conteo de los doce Bytes del header.

Aquí inicia la rutina de copiado del HEADER. Es importante que se entienda como es que se lleva a cabo. En otro doc que anda por ahi se explica paso a paso todo el asm de cartman. En este doc solo se esta explicando de manera general.

COPYHEADER

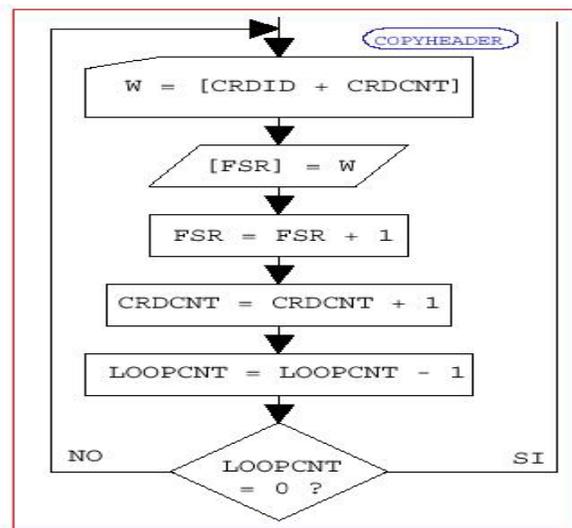


FIGURA 8

Iniciamos cargando en W el valor de CRDID+CRDCNT y lo almacenamos en FSR. Recuerde que el valor de CRDCNT es el valor de las tarjetas gastadas multiplicado por 3 y que CRDID consta de 12 posiciones de memoria donde se almacenará el HEADER. El direccionamiento indirecto por medio de FSR consiste de almacenar datos en la memoria RAM a través del valor de FSR.

INDF va a enviar datos a la memoria de datos (Redundancia) en la dirección que se encuentre apuntando FSR. Esto me costó un poco de tiempo entenderlo, se usan las instrucciones FSR e INDF.

En pocas palabras INDF manda el valor de w a la dirección de memoria RAM que apunta FSR. Si lo entendí mal que alguien me lo diga pliss.

Entonces en este momento FSR estará apuntando en la dirección de CRDCNT (recuerde que CRDCNT=Valor de tarjetas usadas multiplicado por tres) más el CRDID (Que son doce posiciones).

Hay una parte faltante en el diagrama de flujo de Cartman que es la parte donde se escribe la tabla de los headers en la RAM del PIC. Si miramos un poco el asm (No el diagrama de flujo) en la parte final, donde se encuentra la etiqueta CARDID, encontramos dos sentencias fundamentales para la creación de la tabla: `addwf PCL,1` y `retlw`, bueno la primera sentencia nos dice que debemos sumar lo contenido en el registro w y el PCL que es el contador de programa, con esto hacemos que el contador de programa (PCL) se incremente y pueda saltar a cada una de las direcciones del HEADER. El PCL se va incrementando por medio del CRDCNT. Y dependiendo del valor del PCL tendremos el valor de un Byte del Header.

Y con la sentencia `retlw` regresamos de la llamada a la subrutina de CARDID con el valor de un byte del header almacenado en el registro w. Y es en este momento cuando se activa nuestro direccionamiento indirecto

para almacenar en nuestro registro especial CRD_ID el valor del Byte de la tabla.

Bueno, creo que esto esta un poco revuelto pero estoy seguro que después de analizarlo un par de días lo entenderán mejor que yo. ja

Posteriormente incrementamos el CRDCNT, el FSR y el LOOPCNT le restamos 1. Este loopcnt es el que dá la pauta para saber si ya se guardaron en RAM los 12 bytes del header.

En caso de que LOOPCNT sea cero significa que ya se almacenó nuestro HEADER. Por lo cual pasamos a la habilitación de interrupciones.

En el DOC que les mencioné anteriormente también tenemos una explicación detallada de este punto.

La HABILITACION DE INTERRUPTACIONES comienza a partir de este punto y si se dan cuenta podrán observar que la única señal que provoca una interrupción es el CRD_CLK. Expliquémoslo mas a fondo...

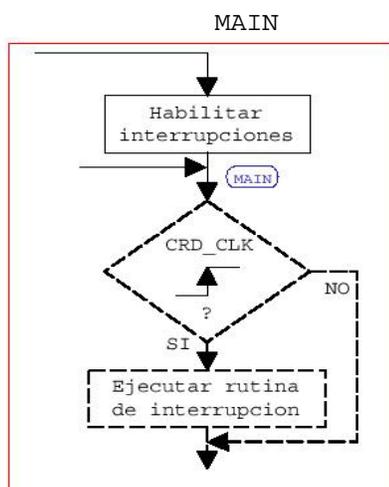


FIGURA 9

Esto es (Según lo veo) un loop infinito en caso de que no se interrumpa la rutina de forma externa. Como podemos observar, la interrupción principal nos la va a dar el CRD_CLK (Fig 9) como lo mencionamos anteriormente, o sea, esto significa que con un flanco de subida de la señal del reloj que nos manda la cabina, tendremos una interrupción, esto es importante ya que el tiempo de estos pulsos de reloj nos dan la relación para seleccionar la velocidad del pic. Por lo tanto llegamos a la conclusión de: Si no sube el CLK no tendremos interrupción alguna y tendremos que esperar a que pase. Recuerde que el pic se puede configurar para recibir señales de interrupción por flancos de subida o bajada por medio del OPTION_REG.

El siguiente paso es ejecutar la rutina de interrupción en la cual van a variar algunos valores importantes que veremos mas adelante. Uno de estos cambios será el valor de FUSCNT (Fig 10) que se encuentra en la DIR 00h de eeprom (Una escritura en la eeprom requiere de checar si ya se termino de escribir).

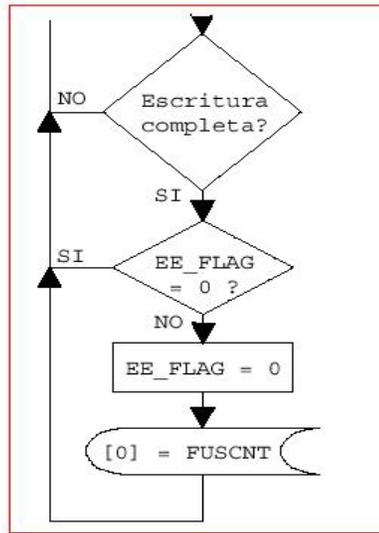


FIGURA 10

Recordemos que el valor inicial cada vez que se recarga la tarjeta, es de DEFAULTFUSCNT= 5. En esta rutina también se checará el estado de EE_FLAG el cual se verá más adelante.

RUTINA DE INTERRUPCION.

Es importante poner mucha atención a esta rutina ya que aquí es donde se realiza la mayor parte de la emulación (El meoyo del asunto). Notese que los parámetros CRD_RST y CRD_WE no son condicionantes para interrumpir el programa principal. Recuerde que el único parámetro para ejecutar una interrupción es CRD_CLK.

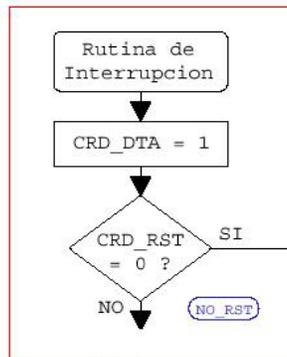


FIGURA 11

Paso uno. ponemos en alto la salida de datos de nuestra tarjeta CRD_DATA=1, después checamos el estado de CRD_RST, esto es para limpiar las variables de inicio tal como BITCNT, POSCNT y cargar FSR con el valor inicial de CRD_ID que es donde se inicia nuestro HEADER y también reiniciar la lectura de datos almacenados en MASKAUX (Aquí se almacena el primer BYTE del HEADER). (Fig 11)

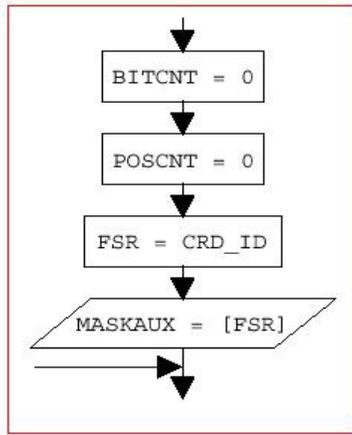


FIGURA 12

Si el CRD_RST es igual a cero entonces nos vamos a la rutina de RESET el la cual ponemos el contador de bits a cero (BITCNT=0), el contador de posiciones en cero (POSCNT=0) este registro es el que se encargará de contar las posiciones de los bits dentro del Byte que se está leyendo y consta de 8 posiciones. También cargamos el FSR con CRD_ID, es decir, apuntamos hacia la dirección CRD_ID de la RAM que es donde inicia nuestro HEADER. Y finalmente almacenamos este valor en MSKAUX que es el registro donde iremos rotando los bits para irlos sacando uno a uno por el CRD_DATA. Ahora seguimos con la rutina de lectura de bits. (Fig 12)

READBIT

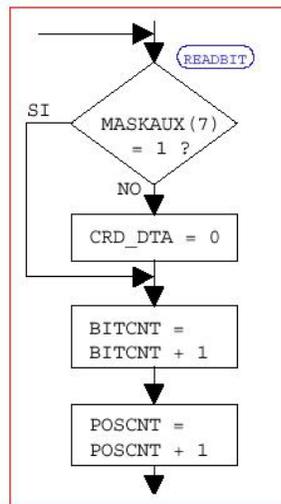


FIGURA 13

Checamos el estado de MASKAUX en el bit mas significativo (7), si es 1 entonces brincamos una instrucción, ya que la siguiente instrucción se encarga de poner la salida de CRD_DATA en cero. (Fig 13)

Observemos que en este punto es cuando tendremos la entrega de datos de nuestro emu a la cabina. En caso de que el bit 7 de MASKAUX sea 0 entonces ponemos la salida de CRD_DATA en cero. (Fig 13)

Posteriormente incrementamos los registros BITCNT (Contador de bits) y POSCNT (Contador de posicion de bit). (Fig 13)

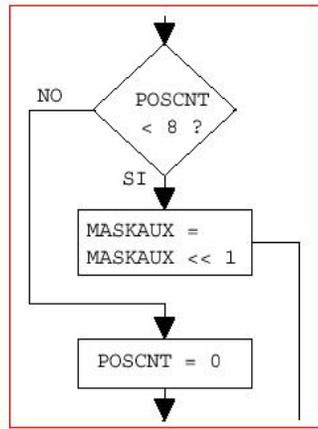


FIGURA 14

Ahora hacemos las comparaciones necesarias para saber se va a hacer: si el contador de posiciones es mayor que 8 (8 bits del Byte que se está leyendo) entonces es tiempo de iniciar una nueva lectura iniciando en la posición 0 en POSCNT, por lo tanto lo ponemos en cero. (Fig 14)

También tendremos que incrementar el FSR en una posición para poder almacenar el siguiente Byte del HEADER en el registro MASKAUX. Y terminamos la interrupción. (Fig 15)

En caso de que el contador de posición siga siendo menor que 8 entonces solamente rotamos MASKAUX a la izquierda (MASKAUX=MASKAUX<<1). Chaleeee.....Que sencillo.. en este momento estamos haciendo que la próxima lectura sea en el BIT siguiente. (Fig 14)

Aquí termina la rutina de interrupción.

Solo debemos esperar a que vuelva a subir el CLOCK que nos envia la cabina para poder realizar la misma rutina.

Ahora solo nos resta analizar el diagrama en caso de que no exista señal de RESET en la tarjeta.

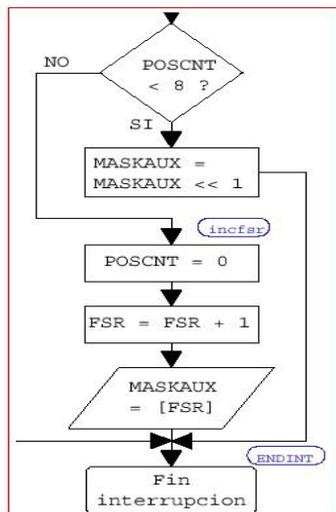


FIGURA 15

NO_RESET

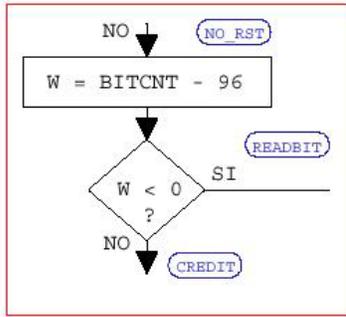


FIGURA 16

En caso de que no exista señal de RST haremos lo siguiente: Checar si el contador de BITS (BITCNT) es menor de 96 entonces hacemos una lectura. Por que 96?? ahhaaaaaahhh... Simplemente porque es el número de bits que tiene el HEADER, y son los que obligatoriamente a fuerzas se deben leer. Recuerde que en esta zona solo se puede leer. La instrucción que aparece en el diagrama de flujo: $w = \text{BITCNT} - 96$ y despues $w < 0$, simplemente nos indica lo que se explico anteriormente. (Fig 16)

Bueno, en caso de que el BITCNT sea menor que 96 entonces nos vamos a la rutina de lectura de BITS (READBIT). Y en caso de que sea mayor de 96, pues nos vamos a la rutina de escritura en la tarjeta. En el diagrama se usa un parámetro llamado FUSCNT, que posiblemente signifique algo así como contador de fusibles (En realidad la memoria interna de la tarjeta contiene fusibles), por lo tanto cuando se hable de fusibles entenderemos que son las unidades de memoria que se van a grabar.

CREDIT

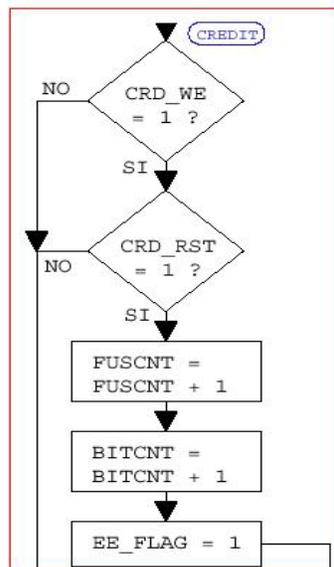


FIGURA 17

Credit hace alusión al crédito restante de la tarjeta y que se inicia a partir del momento en que el HEADER ha terminado de leerse. Primero que nada checamos el estado de CRD_WE (Habilitador de escritura de la tarjeta), si es igual a 1 pasamos a la siguiente instrucción que es la de checar que la señal de RESET no este activada (Recuerde que la señal de RESET se activa con un cero y la de CRD_WE con un uno. (Fig 17)

Espero que puedan seguirme ya que en este punto se hacen algunas ramificaciones del programa. Decíamos que en caso de que el CRD_WE este

activo y el RESET no lo esté, entonces incrementaremos el FUSCNT y el BITCNT, así como poner el EE_FLAG en 1 y terminamos la interrupción. (Fig 17)

Aquí viene algo importante. Se trata de ver el propósito de EE_FLAG, este registro nos sirve solamente para permitir o no la escritura en la eeprom en la dirección 00h. Esta dirección es donde se encuentra almacenado el valor de FUSCNT. Recuerde que el FUSCNT es el contador de fusibles que se van quemando, además que por default ya se encuentra almacenado el 5, que nos indica que ya se quemaron cinco unidades de la tarjeta. Este valor es solamente para que cada vez que se inserte la tarjeta, se tenga con un poco menos del crédito total. Por ejemplo, si se está leyendo una tarjeta de \$50.00 pesos, al insertarla por primera vez, posiblemente se lean \$45.00 (Posiblemente eh).

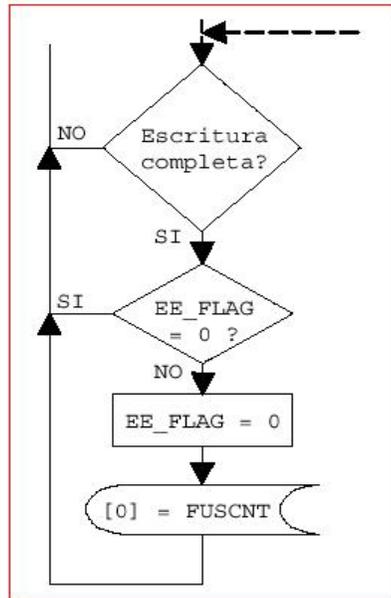


FIGURA 18

Para entenderlo mejor se está poniendo la parte de la rutina MAIN donde nos damos cuenta del propósito de EE_FLAG. (Fig 18) Cada vez que se requiera de escribir o quemar un fusible de nuestro emulador, se incrementará nuestro contador de fusibles y el estado de CRD_DATA no debe cambiar (CRD_DATA=1) ya que una escritura significa poner un uno en la dirección que se este apuntando en la tarjeta o emu. En cambio, si tenemos deshabilitada la lectura y el RESET en la rutina de CREDIT entonces nos vamos a la rutina de NO_WRT

NO_WRT.

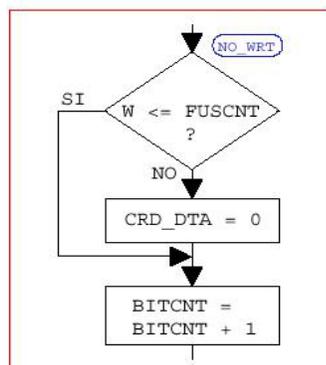


FIGURA 19

En esta sección tenemos cargado en el registro w el valor total de fusibles que se se han ido leyendo o quemando, es decir, si ya estamos en el bit 100, entonces llevamos 4 bits leídos del area de crédito. Pude ser que esten quemados a no, pero lo que importa es lo que tenemos en el registro w. (Fig 19)

Por lo tanto, si w (Unidades de crédito. Creo que les llaman Tokens), es menor o igual a lo que tenemos en FUSCNT (Contador total de fusibles. Recordar que por Default tenemos 5) entonces solamente incrementamos el contador de bits y la salida de datos será 1 (No cambia) por que indica un fusible quemado. Ahora, en caso de que w sea mayor que el FUSCNT (5 por default), significa que ya pasamos de la zona de fusibles quemados por lo que la lectura en este punto debe ser cero (CRD_DATA=0). (Fig 19)

Para finalizar el doc aclaremos que en esta sección (NO_WRT), como su nombre lo indica, no se fundirá ningún fusible pero sí se realizará la lectura.

Conclusión:

El estudio de un emu que ya fue fabricado por otra persona, puede ser el principio del aprendizaje y la investigación para los que apenas se inician. Este estudio solamente se refiere a la parte de programación del PIC para el emu, pero no quiere decir que con esto vas a poder construirte una tarjeta falsa para llamar gratis. Los únicos que podrán realizar el emulador son los que han llegado hasta aquí sin tener absolutamente ninguna duda y además teniendo un poco de conocimientos de programación, un poco de electrónica, que sepan usar algun programador de PIC.

Les deseo mucha suerte y espero que esto sea la base para la realización de mayores proyectos y demostrar que lo que se hace en México se hace con huev..

Para cualquier pregunta y/o aclaración quedo de Ustedes
Muy atentamente

Illan ivanovich 2002.





La mente de un Phreak
por o0ShellGhost0o

¿Qué hay en la mente de un Phreak? ¿Qué retorcidos pensamientos tendrá?
¿Por qué actúan como lo hacen? Lo cierto es que nadie es igual, pero si existe cierto patrón de conducta entre la mayoría de los phreaks y es de lo que hoy les voy a comentar.

¿Qué es un Phreak? Creo que esa pregunta ya no tiene caso responderla, supongo que todos los que están leyendo esto ya lo saben, sin embargo si quiero dejar algo bien claro, un phreak no busca realizar llamadas gratuitas, si no aprender de los sistemas de telecomunicaciones y si, en varias ocasiones nuestros experimentos nos conducen a hacerlas pero ese no es el fin principal.

Pero ¿por qué esforzarse tanto en aprender eso? Es algo que nos nace, muchos de nosotros empezamos en esto por nuestra pasión por la electrónica, la computación y los sistemas digitales. El teléfono es el mayor invento de nuestros tiempos, es una herramienta formidable. Nos esforzamos tanto en entender esta herramienta porque tiene cierta belleza que nos atrae enormemente a ella.

Y bien, ¿cuales son los objetivos de un phreak? A corto plazo pueden ser realizar un emulador, encontrar un pbx, aprender algún estándar de señalamiento como SS7, modificar un celular, etc... pero todos tenemos el mismo objetivo final en mente: Saber más que los demás, más que lo que los investigadores que realizaron esos sistemas saben.

Quizás suena algo egocéntrico, hasta cierto punto narcisista, pero en realidad ese deseo es lo que marcara la diferencia entre los mejores y el resto...

Muchos de nosotros seguimos estudiando en instituciones de nivel superior y estamos conscientes de que la competencia esta muy fuerte allá afuera, sobre todo en estos tiempos en que la globalización deja de ser un pensamiento y se convierte en una realidad tangible.

Todo lo que aprendamos fuera del aula nos ayudara a alcanzar niveles que no nos seria posible alcanzar de quedar satisfechos con los escasos conocimientos que recibimos por parte de nuestros maestros.

Estas investigaciones que realizamos por lo general son de manera individual, dando a conocer los hallazgos y las dudas que salgan durante el estudio en foros especializados en temas referentes a electrónica o telefonía.

Pocos son los que se conocen a un nivel intimo o personal, la mayoría se conoce por sus alias del foro o del chat. Incluso si por ejemplo están desarrollando un proyecto juntos o alguna investigación en equipo, por lo general los integrantes se encuentran a cientos de kilómetros uno de otro.

Este anonimato, que poco a poco nos lo han ido quitando las compañías que controlan las nuevas tecnologías, es indispensable ya que aunque nosotros no tengamos en mente ánimos de lucro o de causar daño alguno, las autoridades nos ven con diferentes ojos.

Para nosotros un emulador es un aparato con el cual podemos simular el funcionamiento de una telecard, es una oportunidad para aprender a

programar microcontroladores y para aprender mas sobre el sistema telefónico público que se maneja en nuestro país; para las autoridades es un artefacto utilizado para robarle miles de millones a las compañías telefónicas (si no me creen busquen en google el articulo que publicó el periódico Español 'El Mundo' sobre este tema).

¿Pero que hay del mundo exterior? Por lo general los phreaks somos personas poco sociables y muy selectivas al escoger amistades. Sin embargo esto no significa que no salgamos a divertirnos, muchos de nosotros somos aficionados a la música electrónica y a los raves.

Muchos de nosotros tenemos novias y amigos, salimos y tenemos vidas normales, claro que primero es lo primero y para nosotros es más importante terminar un proyecto a salir a tomar unas cervezas a la esquina con el grupo de holgazanes de la cuadra, es más importante aprender un nuevo lenguaje de programación a salir a ver la nueva película.

En clases somos por lo general de los mejores estudiantes, con un promedio no tan alto pero elevado, por lo general nos atraen los clubes de computación, ajedrez, tecnología y demás. No pertenecemos a la sociedad de estudiantes ni tampoco somos los más populares, pero somos los que llevamos los proyectos más interesantes.

Nos interesa más la comodidad a la moda, no nos dejamos llevar por lo que la masa piensa.

Como verán un phreak es mucho más que una persona que hace llamadas gratuitas, vivimos con un pensamiento hacktivista y en algunos caso lo empujamos hasta el limite.

Ser phreak es una ideología, es un estilo de vida.

Con esto concluyo este pequeño texto sobre la mente de los phreaks, espero les haya gustado, recuerden postear sus comentarios en los foros de MHM. ¡Hasta el próximo numero!

o0ShellGhost0o



Despedida:

¿Qué les pareció este número? Sin duda alguna el mejor numero que hemos lanzado hasta el momento.

Espero que les haya entretenido además de educado, o que por lo menos hayan pasado un buen rato leyendo la revista phreak de México.

Para el próximo número esperamos tenerles lista una sorpresa que estamos preparando, además de los textos y tutoriales para el mundo underground mexicano. Así que estén muy pendientes.

¡Saludos y hasta la próxima!

--oSUKARu--



Logos que quedaron finalistas.