LECTOR DE TARJETAS para teléfono

Otro de los gusanillos que despertamos todo curioso a las nuevas tecnologias, es saber que se esconde tras una tarjeta de plástico. En los últimos años, este tipo de tarjetas denominadas de pre-pago o Smarcards están siendo empleadas tanto para servicios pre-pago telefonicos, GSM como para la televisión de pago. A veces se trata de una simple memoria y otras de un sofisticado microprocesador. Pero en esta ocasión y como dice el dicho, empezaremos por el principio. Así, conoceremos a continuación que es una tarjeta prepago de solo memoria.

Cada vez se utilizan más las tarjetas de plástico que llevan en su interior insertado un microchip, para todo tipo de aplicaciones y en particular como una avanzada forma de pago. Tal es el caso de las llaves de pago de un canal de televisión codificado, de las que existen multitud de ellas ya en toda Europa o el caso de las tarjetas de pre-pago telefónicos. Sin olvidarnos por supuesto de las empleadas en entidades bancarias o las futuras tarjetas de plastico, de la seguridad social o el DNI en nuestro país.

Estas tarjetas inteligentes, tienen la misma forma y dimensiones que las mencionadas anteriormente, las emitidas por las entidades bancarias, pero lo especial de éstas reside en introducir en su espesor, de aproximadamente 0,76 mm, un microchip (en la mayor parte los casos una memoria EEPROM capaz de ser leída y programada a través de unos contactos, normalmente dorados, por medio de un conector especial. Esta técnica recibe el nombre de « Chip On Board «.

A menudo se nos quiere presentar estas tarjetas como verdaderas fortalezas electrónicas y eso no es así. En su defecto, hay que mencionar que existen normalizadas tres grupos de tarjetas de pago, atendiendo a la función que realiza su microchip.

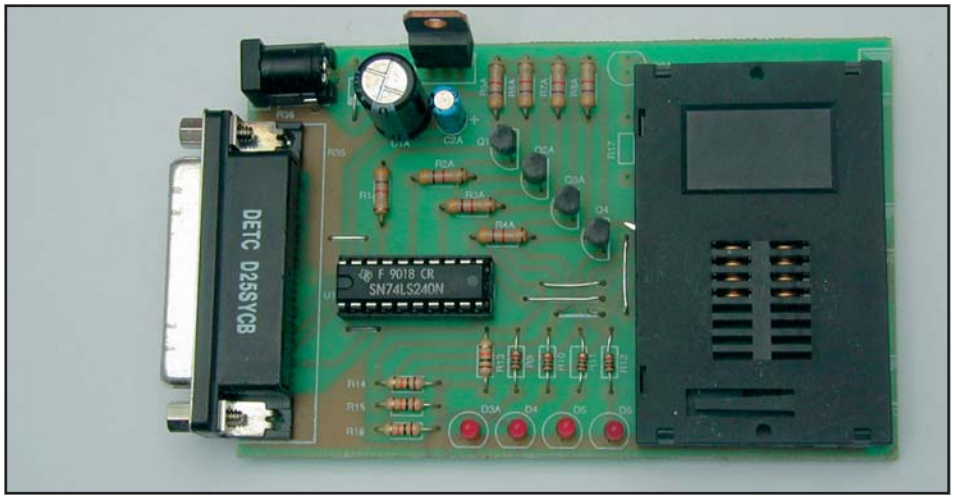
+ Tarjetas simples de memoria,
+Tarjetas personalizadas de memoria
+ Tarjetas con micropocesador (uP).

Como su nombre indica el primer grupo hace referencia a simples tarjetas con una cierta capacidad de memoria sin ninguna protección lógica, en los que se puede leer y escribir informacion con el equipamiento apropiado.

Tecnológicamente estas tarjetas se realizan con EEPROM y son reciclables, es decir se pueden regrabar. Su utilización o uso está restringido a parcelas de la industria o servicios donde la seguridad no sea un factor primordial. Su capacidad generalmente es del orden de algunos kilobits.

Las tarjetas personalizadas de pago deben tener al menos uno de estos tres sistemas de protección, realizados en lógica cableada sin la seguridad que conlleva el uso de un microprocesador.

*** Zona de protección en escritura, previa destrucción de un fusible.**
*** Zona protegida en escritura y lectura por un código secreto " PIN: número de identificación personal" dado por el portador de la tarjeta.**
*** Bloqueo de la tarjeta después de tres intentos de PIN erroneos.**



*** Presencia de un código emisor.**
Dos tecnologías coexisten en este grupo:
*** EPROM protegidas mediante resinas opacas a los rayos ultravioletas "UV".**
*** EFPROM reprogramables eléctricamente.**

Las capacidades de estas tarjetas generalmente son inferiores o 1 Kilobit aunque en la actualidad se están llegando a capacidades de hasta 4 Kilobits. La estrella de este grupo es la EEPROM de 256 bits con una zona de 96 bits protegida confra escritura por la destrucción de un fusible.

Las tarjetas con microprocesador son lo no va más en tarjetas de pago, conteniendo varios sistermas de protección.

*** Zona protegida en escritura o en escritura y lectura por un Codigo secreto emisor.**
*** Zona protegida en lectura y escritura por un código secreto portador "PIN ".**
*** Bloqueo de la tarjeta después de varios intentos de códigos secretos erróneos, pero con posibilidad de rehabilitación por el organismo emisor.**
*** Algoritmos criptográficos " Data Encryption Standard " para asegurar la transferencia de datos.**

Estas tarjetas que poseen microprocesador interno son realmente «duras« de abrir, sin embargo en cuanto a las tarjetas desechables, su resistencia en cuanto a la modificación de la información contenida, resulta bastante vulnerable.

Este podría ser el caso de las tarjetas de prepago utilizadas por las compañías de teléfono de todo el mundo. Por el contrario, esta característica no quiere decir que sean realmente vulnerables al 100%, ya que poseen bits que han sido protegidos en fabrica contra escritura, por fusión de un fusible interno.

En cualquier caso, al ser estas tarjetas ni mas ni menos que una EPROM interna de 256 bits, para recargar esta tarjeta habría que poner a cero todos los bits consumidos, lo que en el caso de la EPROM, esto equivaldría a borrar todo el contenido de la memoria y por consiguiente los 96 bits del fabricante.

Seria un pecado no experimentar con este tipo de tarjetas, aunque sólo sea para leer el contenido de ellas de manera

experimental. Otra aplicación que no sea la simple lectura de la tarjeta quedará como responsabilidad del usuario final. En este artículo lo que pretendemos es experimentar con este tipo de tarjetas y naturalmente dar a conocer que hay dentro de ellas y como funcionan.

Ademas podemos decir por otra parte que cada tarjeta sometida a experientación ha sido previamente comprada, por lo que no estaremos violando en absoluto la legislación correspondiente.

Es un secreto a voces que este tipo de tarjetas sólo llevan una EPROM de 256 bits accesibles al exterior a través de un puerto serie.

Asi los primeros 96 bits están programados en fabrica con unos datos de autoidentificación protegidos por la fusion de un fusible una vez grabada esta informacion. De los 96 primeros bits, los 8 primeros indican el grupo de tarjeta que es, existen varios grupos de tarjetas, los 8 bits siguientes siempre son 0000 0011, en este grupo de tarjeta, los últimos 8 bits del grupo de 96 nos indican el número de unidades que tiene nuestra tarjeta.

En un principio aparecieron de 40, 50 y 120 unidades, en la actualidad solo se comercializan las de 50 y 120 unidades, que por supuesto tendrán valores de credito diferentes. Los 50 bits siguientes, todos a **" 1 ",** corresponden a las 50 unidades de nuestra tarjeta, así si fuera de 120 unidades habría 120 unos. El estado de estos bits a « 1 « indica que son unidades gastadas por lo que nuestra tarjeta refleja que esta vacía.

Después del número de unidades existen 10 bits más que son utilizados en fabrica para algún tipo de control.

A parte de los últimos 8 bits que, cuando están todos a " 1 " indican que una tarjeta esta vacia, todos los demás bits están a **« 0 «** y son estos bits los que se pueden llevar a estado « 1 « para diversas aplicaciones que ya iremos desvelando en próximos números de nuestra revista.

Esta claro que habría menos bits a « 0 « si nuestra tarjeta hubiera sido de 120 unidades o por el contrario habría 10 bits más a **« 0»** si fuera de 40 unidades.

De modo que cuando nosotros insertamos una de estas tarjetas en una cabina telefónica, la unidad central " CPU ", hará que nuestra tarjeta transmita los primeros 96 bits de control y autoidentificación que podrán variar cada cierto tiempo si ello es necesario, para medidas de seguridad, por supuesto inmediatamente despúes de que se a comprobado la correcta identificacion de la tarjeta, se leerán los distintos bits y la pequeña pantalla de la cabina indicará la cantidad de crédito que queda en la tarjeta.

Indudablemente despúes de esto y tras marcar el número de teléfono, la unidad de proceso interno de la cabina ira descontando unidades de nuestra tarjeta, es decir, transformando en 1 todos los «0« no consumidos, por medio de la "quema" de celdas.

Tras esta detallada explicación y a la vez rápida podemos estudiar el circuito propuesto para leer unicamente este tipo de tarjetas. Pero antes, queremos que conozcan una de estas tarjetas en su forma física.

Las funciones de cada pin/out son de la forma que a continuación se detalla:

* **Pin 1: Vcc. Tensión de alimentación de 5v para lectura y 21v para escritura.**
* **Pin 2: Read/Write Control de lectura y escritura.**
* **Pin 3: Clock. Reloj.**
* **Pin 4: Reset. Puesta a cero de la dirección o inicio de las secuencia de salida.**
* **Pin 5: Masa de la tarjeta.**
* **Pin 6: Vpp. Tensión de 21v para la grabación de informacion.**
* **Pin 7: I/O Puerto serie para entrada y salida de datos en el caso de tarjetas con microprocesador, y salida única de datos para tarjetas con EPROM.**
* **Pin 8: Fuse. Pin usado en fabrica para destruir el fusible de seguridad**.

Los datos dados representan a una tarjeta de 8 contactos que ya no se usa, al menos en Telefonía. Actualmente se está trabajando con tarjetas de 6 contactos, como las que sigue;

* **Pin 1: Vcc. Tensión de alimentación de 5v para lectura y 21v para escritura.**
* **Pin 2: Read/Write Control de lectura y escritura.**
* **Pin 3: Clock. Reloj.**
* **Pin 4: GND. Masa de la tarjeta**
* **Pin 5: Reset. Puesta a cero de la dirección o inicio de las secuencia de salida.**
* **Pin 6: I/O Puerto serie para entrada y salida de datos en el caso de tarjetas con microprocesador, y salida única de datos para tarjetas con EPROM.**

Después de ver las funciones de cada pin/out, ha llegado el momento de leer una de estas tarjetas. En nuestra experiencia leimos una tarjeta de 250 Ptas con Lectar un Soft especifico para esta funcion y con TLector, otro Soft de gran calidad. Con este último se obtuvo la siguiente lectura;

##########################
Contenido
##########################

[000]: 11100000 00111100 00110001 01000001 —> E0-3C-31-41
[032]: 10111000 01000101 01010101 11000000 —> B8-45-55-C0
[064]: 00000000 00000000 00000111 01111111 —> 00-00-07-7F
[096]: 00000011 11111111 11111111 11111111 —> 03-FF-FF-FF

##########################
Interpretacion
##########################

Pais: España
Tipo: G+D
Valor: 100 ptas
Nº Serie: 12076373

Esta lectura es totalmente acertada excepto en la cantidad monetaria de la misma. Todos los valores indicados son los correspondientes a los primeros 96 bits de fabricante. Con Lectar sin embargo si se obtuvo el valor monetario correcto, pero no el número de serie. Esto es porque el Software fue creado para tarjetas de 8 contactos y actualmente se está trabajando con tarjetas de 6 contactos, por lo que se deduce que algo mas habra cambiado. Sin embargo con Lectar en conjuncion con Deftar se obtuvo lo siguiente;

```
01 [001..008] 10110100 B4...Checksum
02 [009..016] 01111000 78...Cód. de Tarjeta Teléfonica
03 [017..024] 01100010 62
04 [025..032] 10000011 83
05 [033..040] 00110000 30...Fabricante
06 [041..048] 10001010 8A...Número de serie
07 [049..056] 10101011 AB
08 [057..064] 10000000 80
09 [065..072] 00010100 14...Valor de tarjeta
10 [073..080] 10001010 8A
11 [081..088] 00001110 0E
12 [089..096] 11111110 FE...País:España
13 [097..104] 00000111 07
14 [105..112] 11000000 C0...Comienzo Zona descuento
15 [113..120] 00000000 00
16 [121..128] 00000000 00
17 [129..136] 00000000 00
18 [137..144] 00000000 00
19 [145..152] 00000000 00
20 [153..160] 00000000 00
21 [161..168] 00000000 00
22 [169..176] 00000000 00
23 [177..184] 00000000 00
24 [185..192] 00000000 00
25 [193..200] 00000000 00
26 [201..208] 00000000 00
27 [209..216] 00000000 00
28 [217..224] 00000000 00
29 [225..232] 00000000 00
30 [233..240] 00000000 00
31 [241..248] 00000000 00
32 [249..256] 00000000 00
   FF
```

Los valores indicados son el resultado de ser tratados con Deftar, el segundo Soft de Lectar, con el que se puede modificar el contenido de una tarjeta, para despues escribir en la tarjeta con Lectar. Obviamente lo que no se puede hacer es recargar una tarjeta ya gastada.

EL PEQUEÑO MANUAL

Para realizar todos los pasos anteriormente descritos es necesario conocer al menos, como funcionan Lectar Pro y Deftar. Ambos programas le permitirán conocer el contenido de una tarjeta de teléfono con el fin de conocerlas mas de cerca. Nada mas iniciar Lectar Pro, el lector de tarjetas se le mostrara enm entorno de trabajo principal, véase figura 1.

Como se puede ver, el programa consta de funciones básicas que son las siguientes;

- **Lectura**: Pulsando sobre este botón se realiza la lectura de la tarjeta.
- **Análisis**: Esta opción nos permite realizar un análisis del comportamiento de la tarjeta ante diferentes eventos y operaciones de borrado. Tambien nos permite comprobar el adecuado funcionamiento del Hardware.
- **Guardar**: Es posible guardar el contenido de la tarjeta en diferentes formatos. Estos formatos son Binario, Hex o Formato tarjeta entre otros. Esto simplifica su manipulacion posterior.
- **Salir**: Esta funcion es tan sencilla como permitir terminar la ejecución del programa.

Además, a través de la opción *Configuración* del menú *Archivos*, es posible acceder a dos opciones que son muy importantes para la ejecución del programa. En esta ventana, véase figura 2, podemos, por un lado, realizar la inversión en la lectura de la tarjeta, opción indispensable cuando utilizamos el interfaz para el puerto paralelo, y por otro lado tenemos la opción de temporización, necesaria para la ejecución del programa en ordenadores de elevada velocidad de proceso. Si no se emplea el metodo de inversion podremos leer tarjetas sin el uso del Hardware presentado, pero basandonos en el conexionado de la figura 3.

Una vez conectada la tarjeta con el puerto paralelo del PC, ya sea directamente o a través del interfaz, podemos llevar a cabo la operación de lectura de la tarjeta. En este ejemplo, hemos instalado una tarjeta de 1ª generación del fabricante G+D con un valor de 1000 ptas. y un saldo de 60.

Podemos apreciar en la figura 4 como la pantalla principal se expande horizontalmente hasta mostrar el análisis realizado por parte del programa de la memoria de la tarjeta, además de permitir la opción *Guardar* del menú principal.

El programa proporciona el checksum de la tarjeta, el fabricante, el número de serie, el país para la que fue fabricada, el valor de la misma y el saldo actual. Además, analiza las zonas de descuento de la tarjeta indicando el saldo que contienen.

Una vez realizada esta primera lectura, tenemos la posibilidad de realizar un estudio más detallado del comportamiento

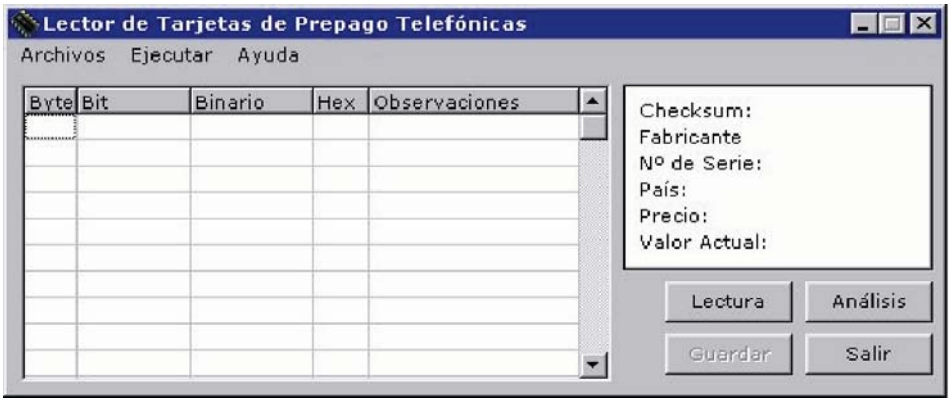


Figura 1

de la tarjeta y el borrado de algunos bits de la zona de descuento en el caso de que la tarjeta sea de 1ª generación y del fabricante G+D.

Estas nuevas opciones aparecen al pulsar sobre el botón de análisis, con lo que el menú principal se expande verticalmente mostrando el aspecto que aparece en la figura 5.

Por un lado, podemos apreciar el contenido de la tarjeta de forma más detallada, separando la zona de descuento de la zona protegida de la tarjeta. Además, también podemos apreciar una serie de 'leds' que nos indican el estado de los circuitos que actúan sobre la tarjeta. Por último, contamos con varios botones cuyas funciones se describen a continuación:

- **Borrar:** Permite borrar el bit o los bits seleccionados, realizando posteriormente la lectura de la tarjeta.
- **Lectura**: Realiza la lectura de la tarjeta.
- **Cerrar:** desactiva la expansión tanto horizontal como vertical del menú principal.

Figura 2

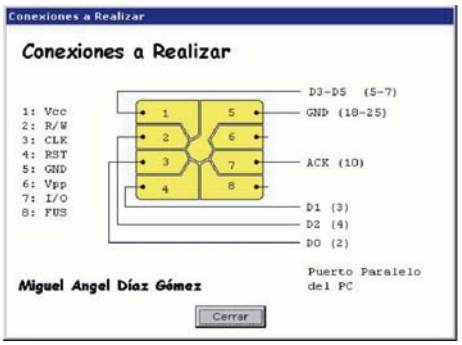


Figura 3

- **L.S.A.** (Lectura Sin Apagar la tarjeta). Realiza la lectura de la tarjeta pero al finalizar mantiene activo los circuitos.
- **L.S.R.** (Lectura Sin Reset): Lee la tar-

Figura 4. Expansión horizontal de la pantalla principal

Figura 5. Ampliación vertical de la pantalla principal

jeta sin antes realizar una operación de reset.

- **B.S.L.** (Borrado sin lectura): Borra el bit o los bits seleccionados pero no realiza una posterior lectura de la tarjeta.
- **Vcc ON/OFF**: Activa/Desactiva el circuito Vcc (ISO 1).
- **RST ON/OFF** : Activa/Desactiva el circuito RST (ISO 4)
- **R/W ON/OFF**: Activa/Desactiva el circuito R/W (ISO 2)
- **CLK**: Produce un impulso de la señal de reloj
- **CLK ON/OFF**: Activa/Desactiva el circuito CLK (ISO 3)
- **L.H.B.** (Lectura Hasta el Bit): Realiza la lectura hasta el primer bit seleccionado, sin incluirlo.
- **I/O** : Visualiza en la barra de leds el estado del circuito I/O (ISO 7).
- **Leer**: Lee el siguiente bit de la tarjeta y muestra el resultado en la casilla anexa.
- **Reset**: Produce una operación de reset en la tarjeta.
- **R**: Produce la puesta a cero del contador de segundos.
- **E**: Habilita/deshabilita el contador de segundos.

Pulsando en cualquier bit '0' de las zonas de visualización del contenido de la tarjeta, activamos la opción de *borrar,* además de activar *B.S.L.* y *L.H.B.*. Si pulsamos sobre el botón *borrar*, el programa procederá a ejecutar una acción de borrado sobre el bit marcado, la cual será efectiva únicamente si este bit se encuentra en la zona de descuento. Después leerá el contenido de la tarjeta para comprobar si se ha llevado a cabo el borrado del bit y activará un contador que mostrará los segundo que van transcurriendo con el fin de contabilizar el tiempo máximo que el emulador es capaz de conservar el estado del bit borrado antes de que se resetee debido a la falta de alimentación. Se ha implementado esta opción para comprobar que el emulador guarda el contenido de la tarjeta mientras no existe alimentación por parte del lector.

Hasta aquí se ha mostrado como utilizar el programa Lectar Pro, que evidentemente ha sido extraido de la propia página donde se ofrece el Programa que es totalmente Freeware. En este sentido se agradece a Miguel Angel Díaz Gomez tan elaborada pagina y como no la creacion de dicho Software.

Este programa es capaz de calcular el contenido de las tarjetas de los fabricantes Oberthur, Gemplus y G+D con un valor de 1000, 2000 y 2100 ptas. pudiendo elegir el saldo y el número de serie de estas tarjetas. Además el contenido de la zona gastada se coloca todo a '1' aunque sólo sería necesario poner a '1' el primer bit de esta zona, disminuyendo primeramente la zona de descuento lento de la tarjeta.

La pantalla principal del programa la podemos observar en la Figura 6. Esta primera pantalla nos muestra las diferentes opciones que podemos elegir a la hora de configurar el contenido de la tarjeta (fabricante, valor, nº de serie y saldo) además de una serie de botones que describimos a continuación:

- **Cargar**: Pulsando sobre este botón actualizamos el contenido de nuestra tarjeta "virtual" con el contenido de una tarjeta previamente almacenada.
- **Guardar**: Con esta opción almacenamos en disco el contenido de la tarjeta obtenido a través del programa.
- **Desmenuzar**: Pulsando sobre este botón podremos manipular directamente el contenido de la zona de descuento de la tarjeta.
- **Acerca de**: Esta opción nos muestra la pantalla mostrada en la Figura 1.
- **Salir**: Pulsando este botón terminaremos la ejecución del programa.

Las modificaciones del contenido de la tarjeta virtual se van realizando a medida que vamos seleccionando cualquiera de las opciones de la pantalla principal. También indicar que el saldo ha de ser 0 ó múltiplo de 5 debido a que este valor es el mínimo que podemos descontar de una tarjeta. Si seleccionamos un valor que no cumpla estas condiciones desaparecen los botones *Guardar* y *Desmenuzar* y no se actualizará la tabla que muestra el contenido de la tarjeta.

La opción *Cargar* permite actualizar el contenido de la tarjeta virtual con el contenido de una tarjeta previamente almacenada. El formato del fichero ha de ser cualquiera de los anteriormente descritos con lo que se garantiza una completa compatibilidad con el programa Lectar Pro. Esto es importate a la hora de obtener una tarjeta virtual a partir del contenido de una tarjeta real obtenido con nuestro lector de tarjetas telefónicas.

Una opción interesante es la de *Desmenuzar*. Con esta opción podemos modificar el contenido de la zona de descuento de la tarjeta de una forma directa manipulando los bits que conforman esta parte de la memoria. En la Figura 7 podemos observar la pantalla que nos aparece al pulsar sobre esta opción.

Pulsando en cualquiera de las celdas que nos muestra el contenido de la zona de descuento de la tarjeta cambiaremos su valor de "0" a "1" y viceversa, modificando el saldo de la tarjeta así como el valor hexadecimal del byte afectado. Además se nos muestra las direcciones de comienzo de las zonas lenta y rápida que depende del valor de la tarjeta que hayamos seleccionado.

Ahora ya conocemos tambien Deftar, que una vez mas se ha extraido la informacion de dicha pagina. Para finalizar cabe resaltar que el Hardware presentado aquí está adaptado a las nuevas tarjetas de 6 contactos ya Lectar Pro, asi como a Tlector. Recuerde que cada Soft utiliza Pines diferentes en su funcionamiento. La idea esta en extender el presente Hardware al mayor numero de Soft disponible en la ReD. Pero actualmente Deftar y Lectar Pro, son los Soft mas interesantes.

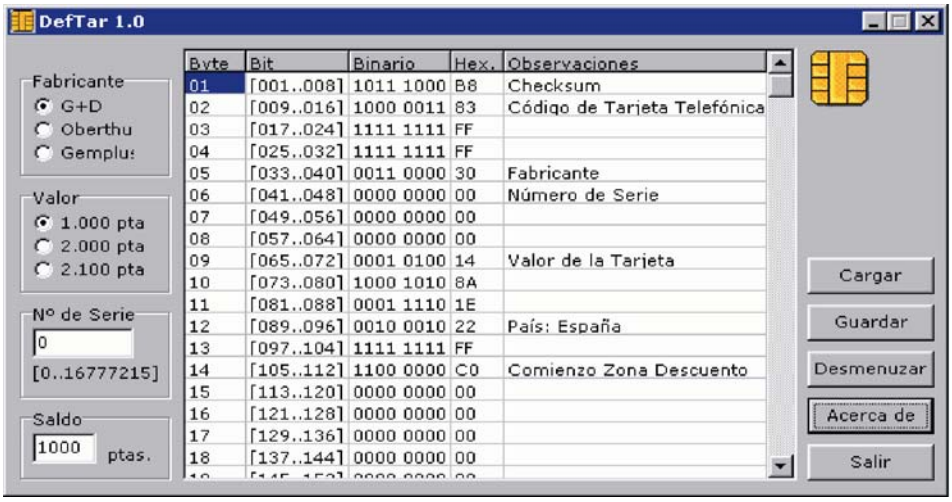


Figura 6. Pantalla principal del programa DefTar en su versión 1.0

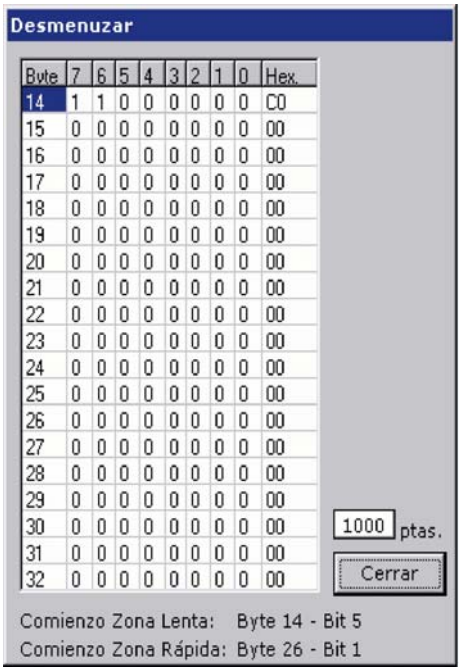


Figura 7. Opción Desmenuzar del menú principal