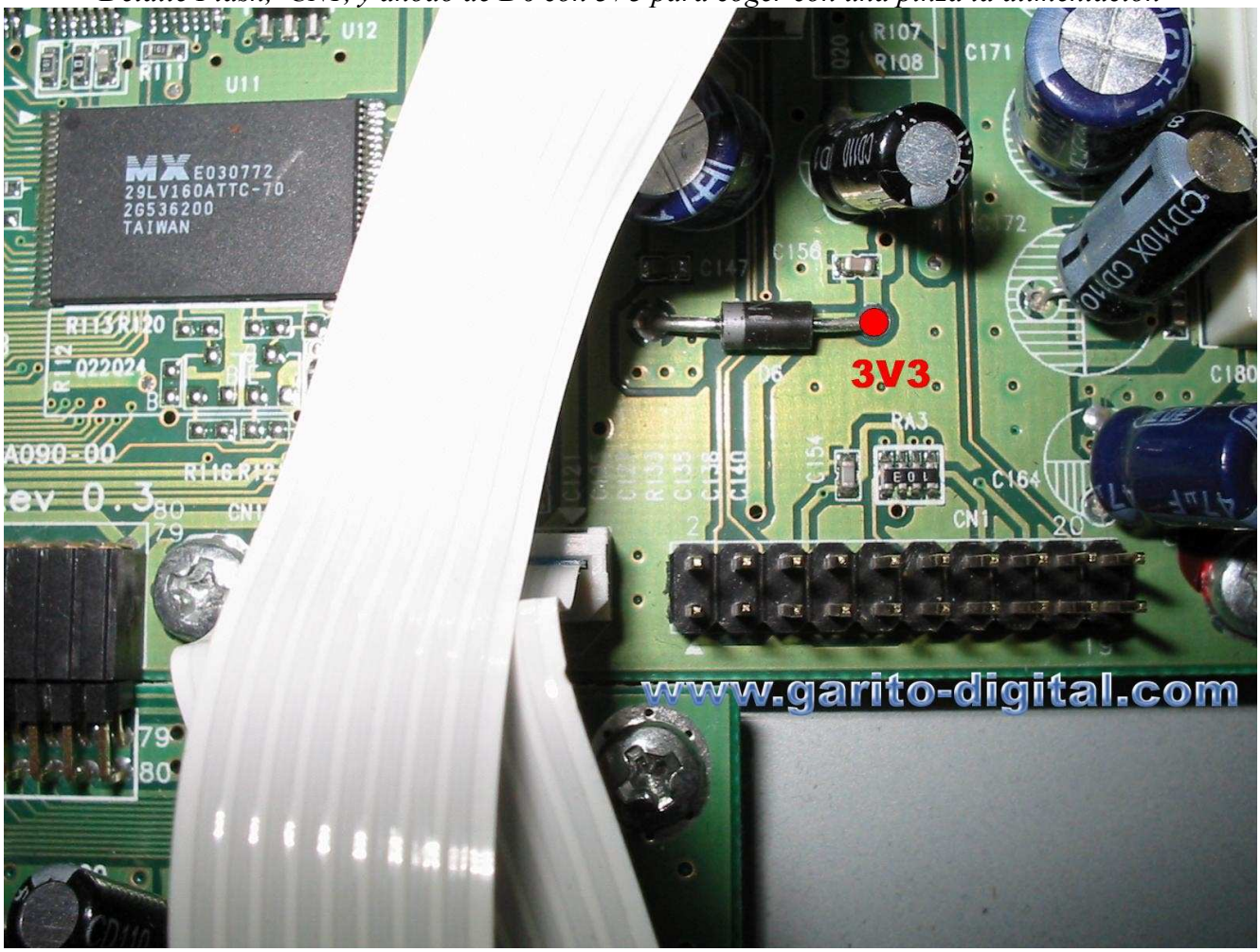
JTAG para FCIS7000 v2

Las pruebas están hechas con un interface Jtag comercial, el de la pila de litio, con cable plano de 20 hilos y conectores FC-20P 1 a 1 en ambos lados. Aunque se puede utilizar un Jtag casero basado en resistencias y sin necesidad de alimentación, que funciona en base a adaptar resistivamente la salida TTL (5V) del ordenador a la requerida CMOS (3V3) por el receptor. Lo he probado y funciona igual, podéis encontrar esquemas por la red y es fácil de construir, aunque a mí, personalmente, me gusta más el que uso por asegurar los niveles correctos independientemente del consumo y asegurar el aislamiento de los equipos.
Os pongo una foto del que yo uso:

1.- Conectar el Jtag con el receptor apagado, si lo habéis cableado bien, el cable rojo (hilo nº 1) debe ir al terminal 1 (tiene un pequeño triangulo serigrafiado en la placa) del conector CN1 del receptor.
En la siguiente página os pongo dos fotos con los detalles:

ES MUY IMPORTANTE TENER LA PILA DEL JTAG EN BUENAS CONDICIONES O USAR LA ALIMENTACIÓN DEL RECEPTOR (POR EJEMPLO, ÁNODO DE D6)

Detalle Flash, CN1, y ánodo de D6 con 3V3 para coger con una pinza la alimentación

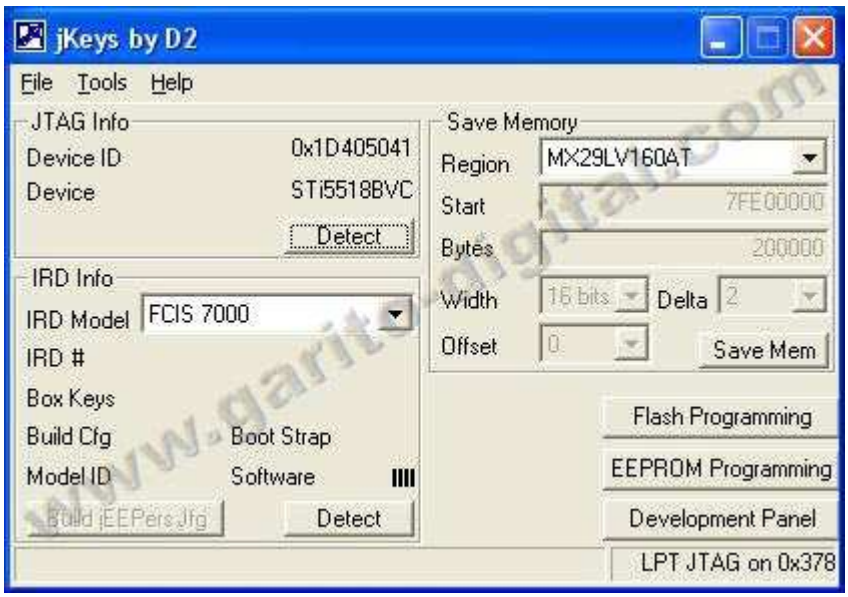


Detalle conexión alineada, hilo rojo al triángulo que señala el pin 1

2.- Encender el receptor con todo conectado, Jtag al LPT1 y Salida al CN1 del receptor, puente del Jtag activado (habilita la alimentación)

3.- Ejecutar el Jkeys proporcionado, hacer clic en preferencias y seleccionar el puerto y dirección de memoria usada (por defecto 0x378), es conveniente que el puerto sea EPP (bios) y use interrupciones si se le asignan. (Propiedades de puerto en el administrador de dispositivos de Windows)

Si todo está bien conectado, el Jkeys reconocerá el modelo de micro, sólo hay que seleccionar el receptor en el desplegable "IRD Model", Y en "Region" el tipo de flash que monte vuestro receptor:

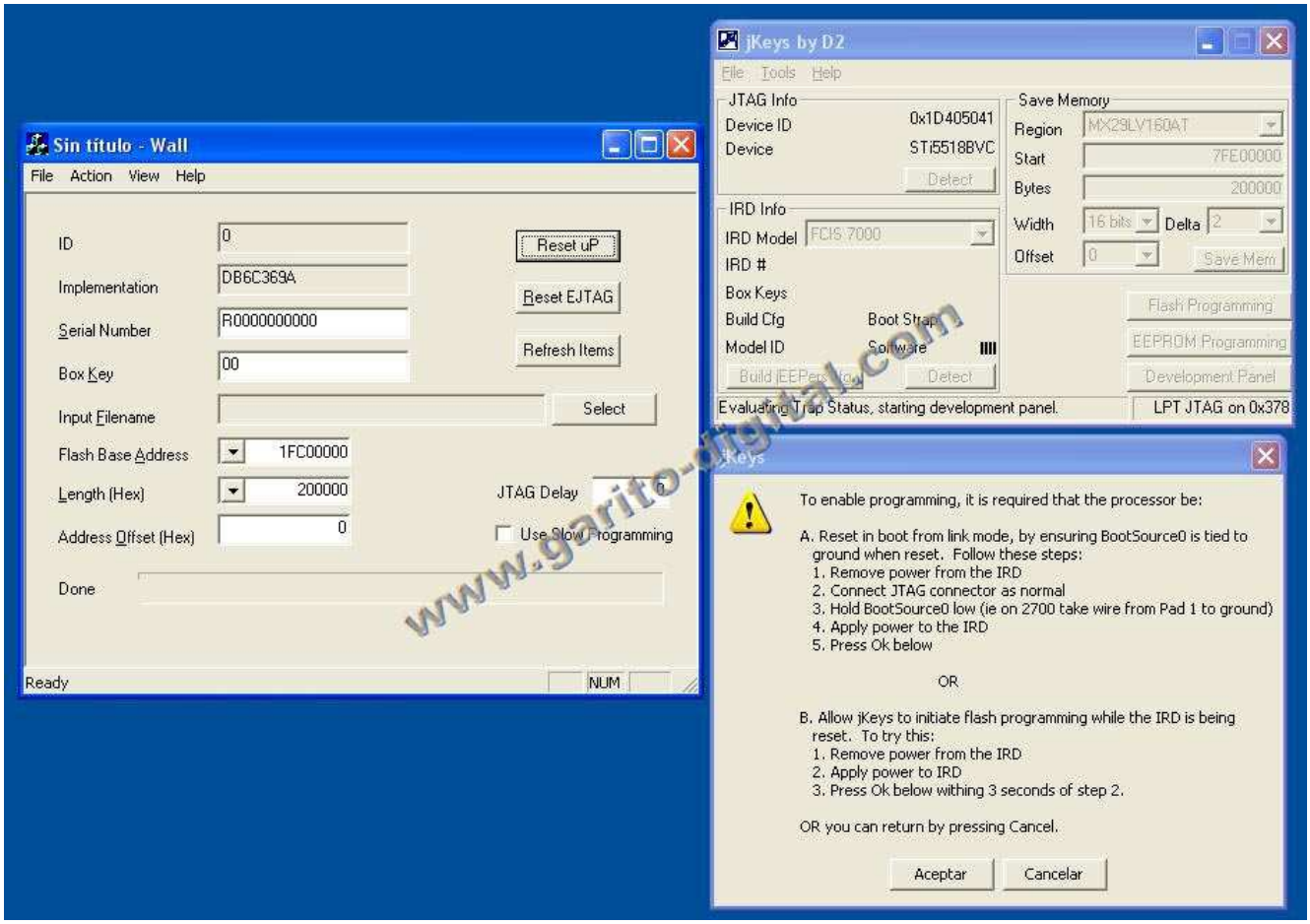


En este momento ya podríamos hacer una copia del firmware pulsando sobre "Save Mem"

4.- Lo siguiente que vamos a hacer va a ser parar la ejecución de código desde la flash, para pasar a modo DCU, hay una rutina especial en esa zona del micro que nos permitirá actuar sobre él con el Jtag.

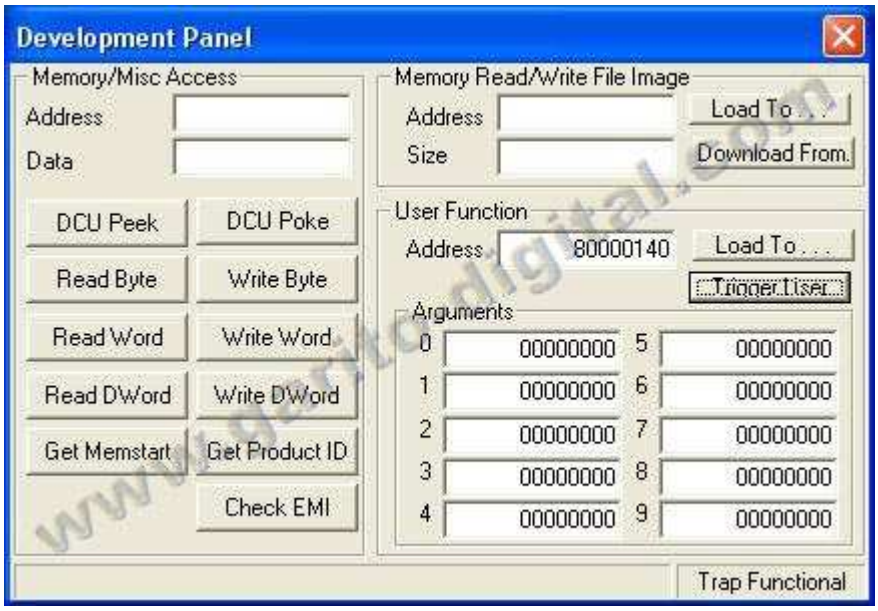
Esto se puede conseguir de diferentes formas, una de ellas es con el jkeys en el momento de arranque, pero necesitamos un boot válido y siempre no va ser así, otra es con un puente hard en la placa del deco, actuando sobre la señal BootFromRom, pero también lo apartamos por arriesgado (aunque hay otros receptores que llevan un "jumper" para eso) , y otra es mediante un programa llamado Wall, que mediante su función Reset MicroProcessor nos permitirá entrar en ese estado, ya que utiliza la señal de reset del Jtag (el jkeys no lo hace)

- Hacer Clic en “Development Panel”
- Seguidamente abrir Wall, os saldrá una ventana de Warning, dadle a aceptar.
- Luego hacer clic en “Reset uP” hasta que el valor del campo “Implementation” no varíe (Volver a ignorar el warning que sale con “Aceptar” cada vez que lo hagamos).
- Ya podemos darle al “Aceptar” del aviso del jkeys y proseguir.



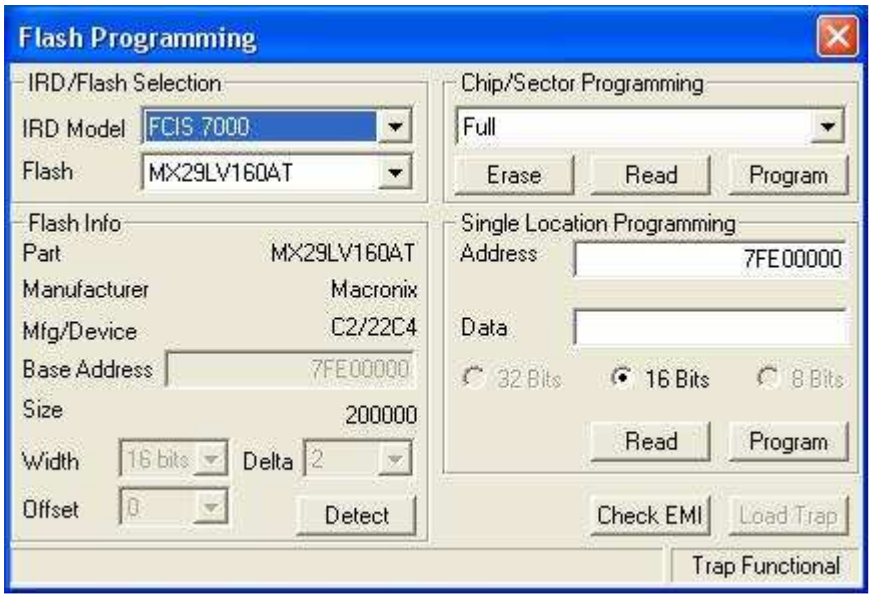
En este momento hemos entrado en la pantalla de “Development Panel”, y vamos a proceder a desproteger la flash para poder escribir en ella:

El método de desprotección depende del tipo de flash que tengamos, y vamos a distinguir entre las Macronix - ST y las Intel, aunque el método para vosotros va a ser el mismo, para ahorraros dolores de cabeza. Todas son de 16Mbits, o sea, de 2 Mbytes, pero varían en la forma de escribir los datos, aunque los fabricantes ya se habían puesto de acuerdo y el patillaje es similar, luego sólo hay que soldar unos cuantos componentes extra en el deco y a funcionar.



Bien, al tajo, ya estamos con la pantalla de arriba abierta, y aquí vamos a cargar en la zona de usuario de la DCU unas rutinas que nos van a ahorrar el tener que ir dando instrucciones por separado:

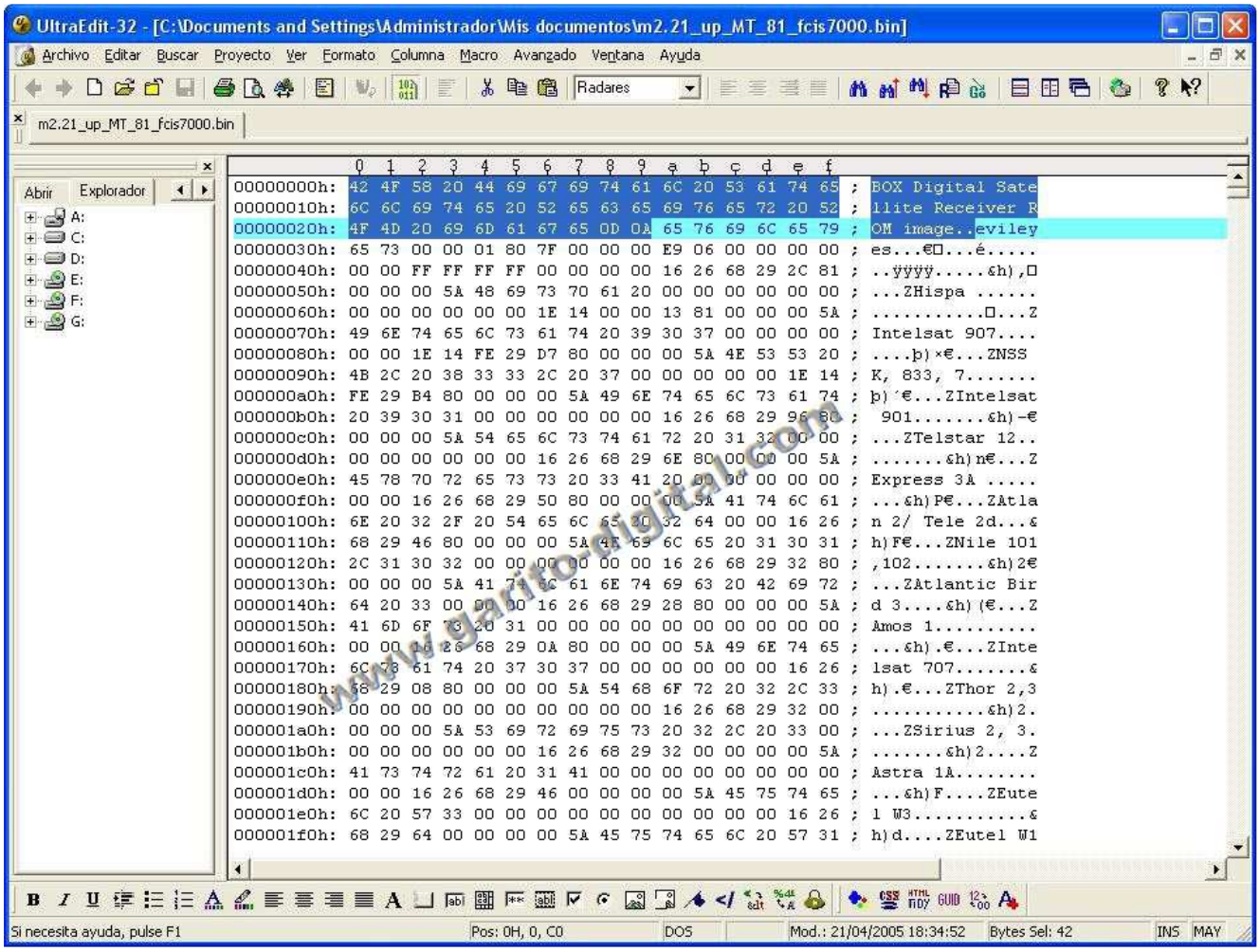
- En el campo "User Function" introducimos el principio de esa zona libre, que puede variar en otras marcas de receptores o modelos del 5518, pero que en el nuestro es 80000140, si alguien se quiere asegurar puede darle al botón "Get Memstar"
- Luego hacemos clic en el botón "Load to…" que hay a su derecha, y cargamos el fichero binario correspondiente a la flash a desproteger, sólo os pongo dos, uno que sirve para las series 29xx160 (Macronix y ST) y otro para la serie 28xx160 (Intel). Bien lo cargáis y le aceptáis.
- Ahora hay que ejecutarlo haciendo clic en "Trigger User", se os llenarán los 8 campos de Arguments a 0, es normal.
- Con esto ya se puede cerrar el Development Panel y pasar a Flash Programming, con lo que si todo os ha ido bien os saldrá la pantalla en la que seleccionaréis el modelo de receptor y automáticamente se pondrá el tipo de flash que monta:



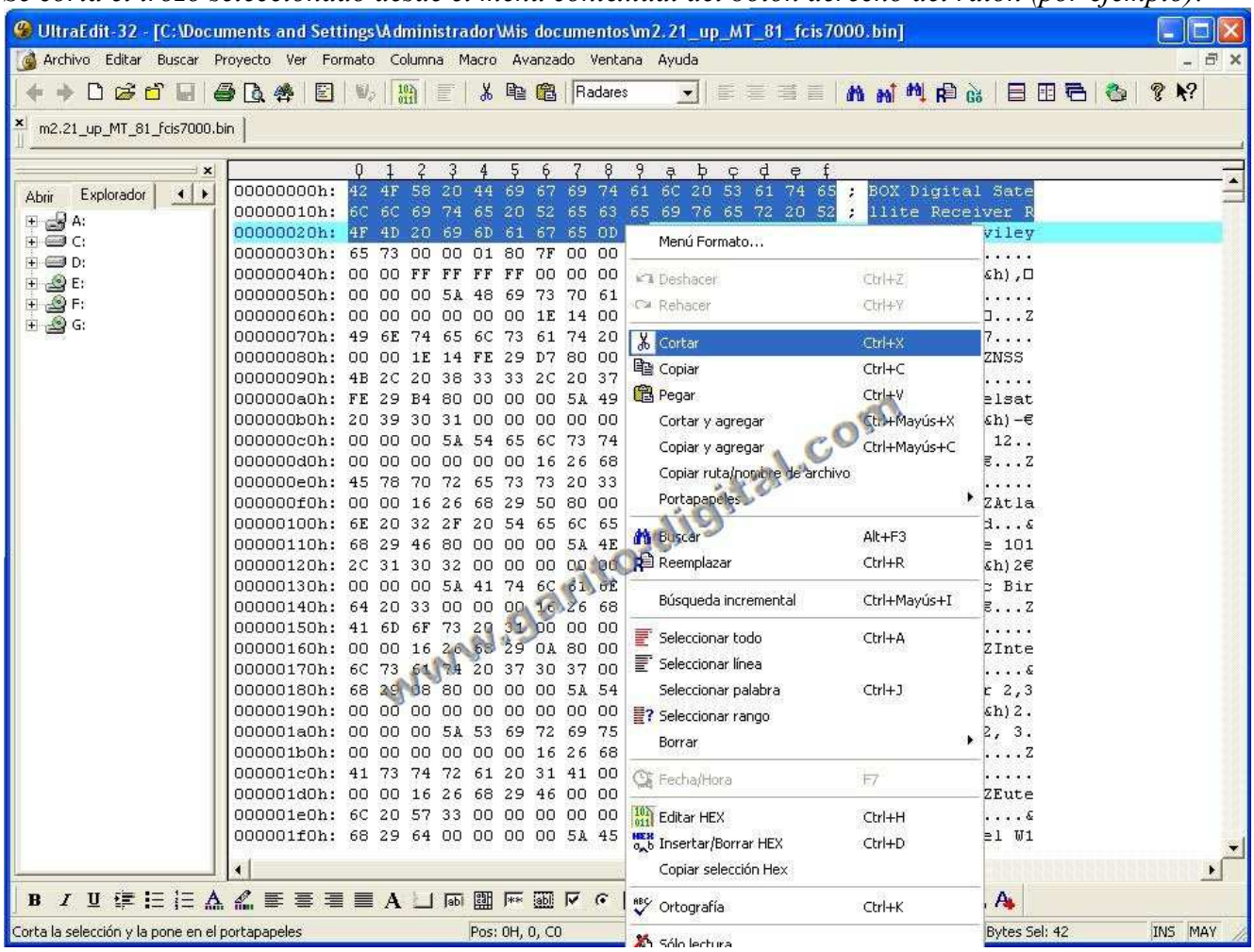
Técnicamente, para introducir un nuevo firm a la flash, primero hay que borrarla, pues este tipo de memorias sólo pueden poner bits a 0, y para ponerlos todos a 1 sólo la función “erase” puede hacerlo. Esto teóricamente, pues luego podemos sobrescribir sin problemas para hacer pruebas y no pasará nada, pero como queremos dejar limpia la flash, lo primero que haremos será borrarla haciendo clic en “Erase” y esperando unos 30 segundos que tarda el proceso.

Llegados al punto de la programación, he de hacer hincapié entre el tipo de receptor y de flash que tengáis.
En caso de que el receptor sea un FCIS7000 de los primeros, ya sea IllusionSat M4 , Galaxis Hispania o Mvision, o sea un Mvision E+ con flash diferente a Intel 28F160, seguiremos el método normal, que os describo a continuación: (los demás, esperen, por favor)

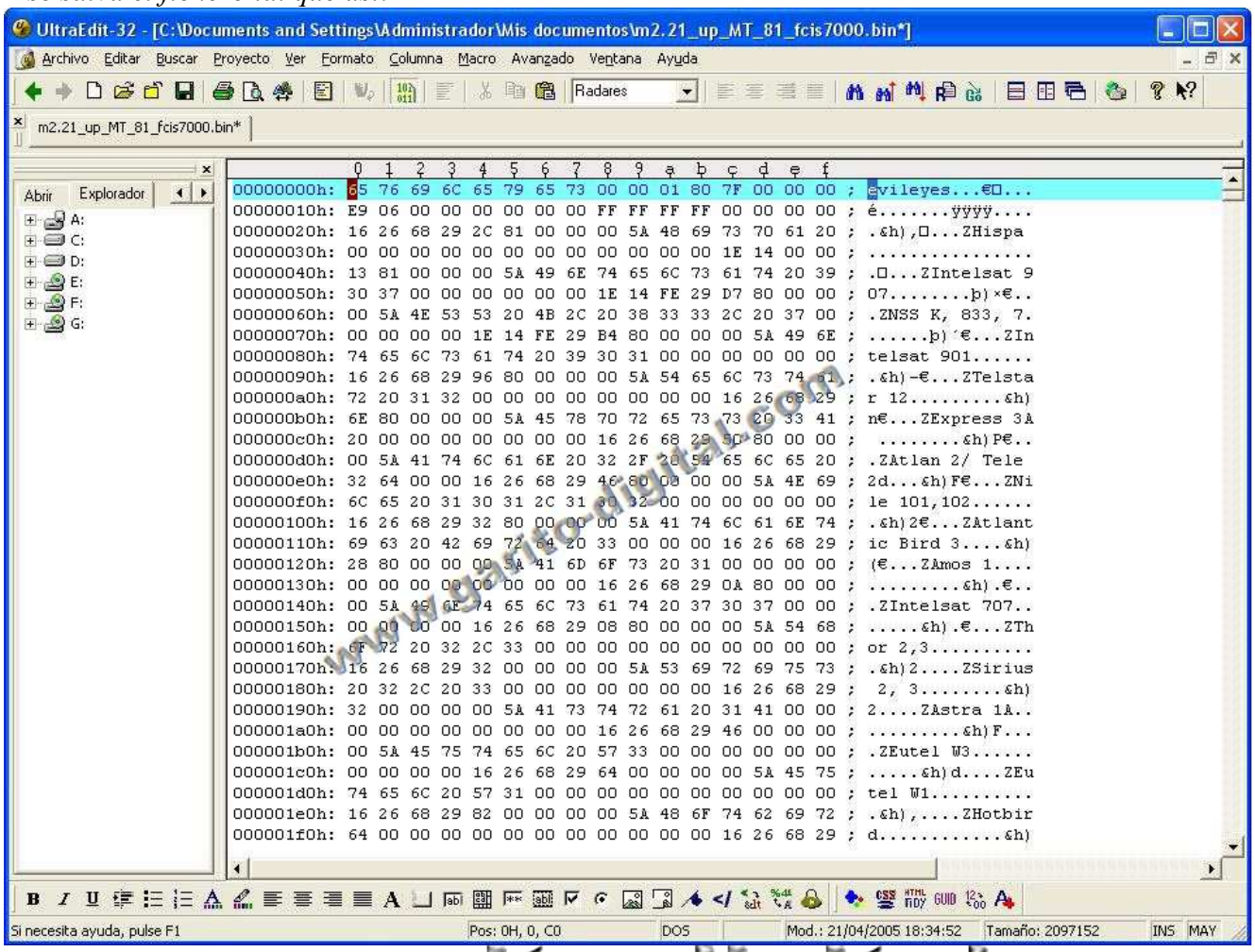
Con la flash ya borrada, sólo nos queda darle a “Program” e introducir el fichero binario del firmware que creáis conveniente, eso sí, si lo habéis bajado de la red y está preparado para introducirse vía puerto serie con el boxloader o el FCISUtils, habrá que quitarle la cabecera de 42 bytes que gasta, utilizando cualquier editor hexadecimal, y sin necesidad de recalcular checksum ni nada más, para ello, se edita y se seleccionan los primeros 42 bytes, hasta donde pone “evileyes”:



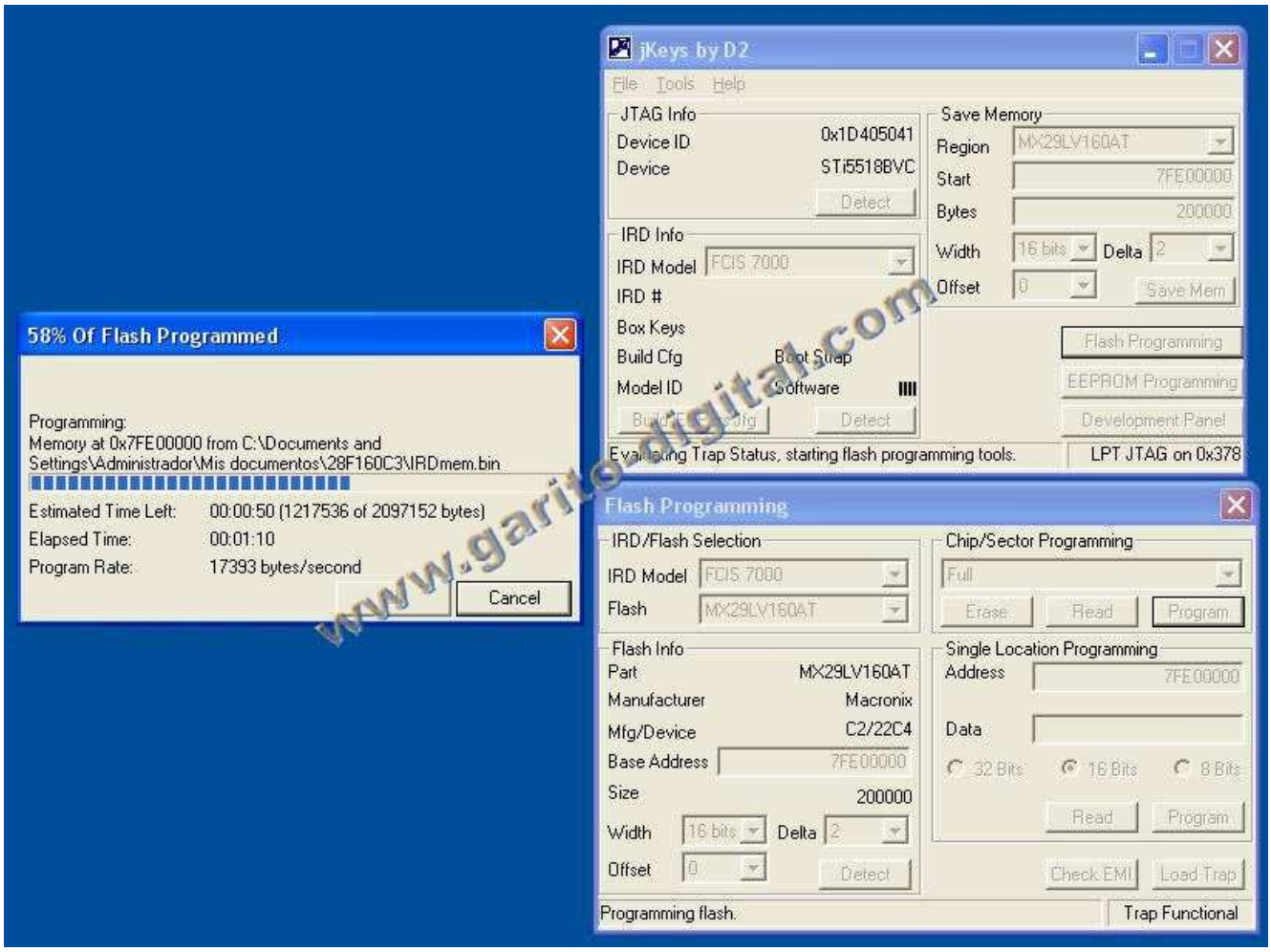
Se corta el trozo seleccionado desde el menú contextual del botón derecho del ratón (por ejemplo):



Y se salva el fichero tal que así:



Con esto ya tenemos un fichero binario de 2Mbytes exactos, preparado para introducirlo en la flash, y empezará a programarlo, tardando unos 2 minutos aproximadamente:



Cuando acabe ya podemos cerrarlo todo y apagar el receptor para volverlo a encender sin jtag ni nada, y revivirá ;-)

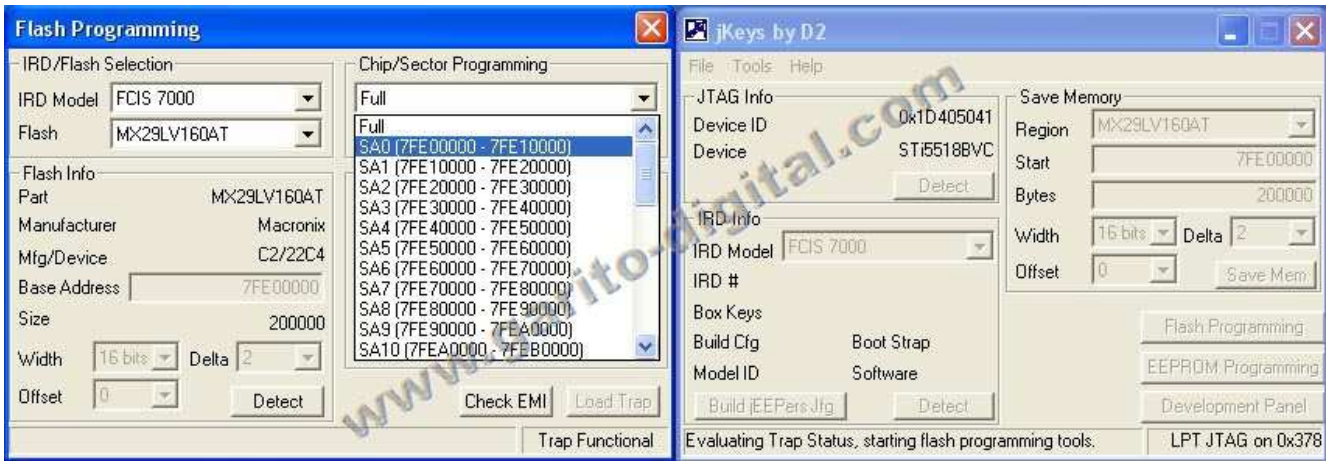
Bien, pasemos al caso de los **Mvision E+** con flash **Intel**:

En este caso, si ya tenéis el receptor muerto, podéis probar el método de arriba a ver "si suena la flauta", pero la experiencia dice que os dará problemas de escritura un montón de veces, así que lo ideal es que intentemos grabarlo a trozos pequeños, para minimizar los riesgos y vuestra desesperación.

Para ello, os he troceado un firmware oficial del E+ en todos los segmentos de los que se compone la flash Intel, o sea en 39 ficheros binarios, que corresponden a cada sector físico y lógico de la memoria.

Evidentemente para grabarlo hay que seleccionar cada vez el sector apropiado antes de darle a programar.

Darle a la flecha del campo de selección "Chip/Sector Programming", y en vez de seleccionar "Full", seleccionar cada vez el sector apropiado, empezando por SA0 y acabando por SA38, y cada vez cargando el fichero binario correspondiente.



Si da error de escritura, volver a intentarlo hasta que lo haga correctamente. He de decir que esto os puede costar horas, así que armaos de paciencia y a darle al botón, que al final se consigue, aún no se ha probado con ningún receptor que se haya resistido, o sea, que intentadlo.

Cuando hayáis acabado con los 39 sectores, ya se puede apagar todo y tendréis vuestro E+ con el firm de fábrica.

TRUCO: el **boot** se aloja en los sectores **37** y **38** solamente, luego si queréis, podéis borrar sólo esos 2 sectores y reprogramarlos, pues puede que el problema solo esté en ellos, y así intentar recuperar luego un **error0.**
Además, el firm oficial que acompaña a este manual, tiene los sectores 27 a 36 vacíos (ambos inclusive), luego si os da muchos errores, podéis obviar estos sectores si antes se ha borrad la flash entera ;-)

Como siempre, leed todo bien y preguntad lo que no entendáis, pues aunque seguramente si estáis leyendo esto vuestro receptor ya está frito, cada cual es el último responsable de lo que hace, y hay que actuar SIEMPRE con sentido común y sin prisas.

Sólo me queda dar las gracias a los compañeros y amigos que me han ayudado con esto, y que han puesto sus receptores a mi servicio para trastear con ellos, con el riesgo de mandarlos a la chatarra por el camino, y que son : **Geppeto**, **fran001**, y **Lara,** sin los cuales no habría podido meterle mano a los E+, o en el caso de Lara, a un oldFCIS7000 con flash Intel, recuperado y sano y salvo siguiendo los métodos del manual.

Un especial saludo a los tres y **GRACIAS**.

Gracias también a Dave por su fabuloso Jkeys, y al creador del Wall, sin los cuales, evidentemente, todo esto nos sería mucho más complicado.

Si alguien necesita aclaraciones, tiene dudas, o simplemente desea comunicarme sus experiencias con el Jtag y nuestro deco, puede encontrarme en…..

www.garito-digital.com

No sabía si lo había puesto ya en algún sitio ;-)

PD.: Los fuentes de los binarios de desprotección, información más técnica e incluso esquemas electrónicos, están a vuestra disposición si alguien se quiere meter más a fondo, pero he pensado que escapaba de las pretensiones de este manual, el que los quiera que se ponga en contacto.

Lethaeus 2006