

Il BLACK Ed Io... o come fare soffrire ad un programma fino a limiti insospettati.

Visto che c'è molta gente che è ancora più persa di me in questo della Scrittura Controllata, mi sono deciso a contarvi le mie esperienze... che quello di contare sé che mi è dato bene. Vada davanti un'avvertenza: questo non è un manuale che vi garantisca nessun tipo di risultato. Semplicemente passerò a raccontarvi le mie esperienze con questo magnifico programma per se a qualcuno lo servisse da aiuto. Di non essere così... per lo meno sicuro che si getta alcune buone risate.

Detto questo mi rimane solo ringraziare al Team per il meraviglioso attrezzo che ci ha facilitato... e ringraziare a tutti quegli amici che si gettano ore perse con me procurando che ogni giorno impari un pochino più... Grazie.

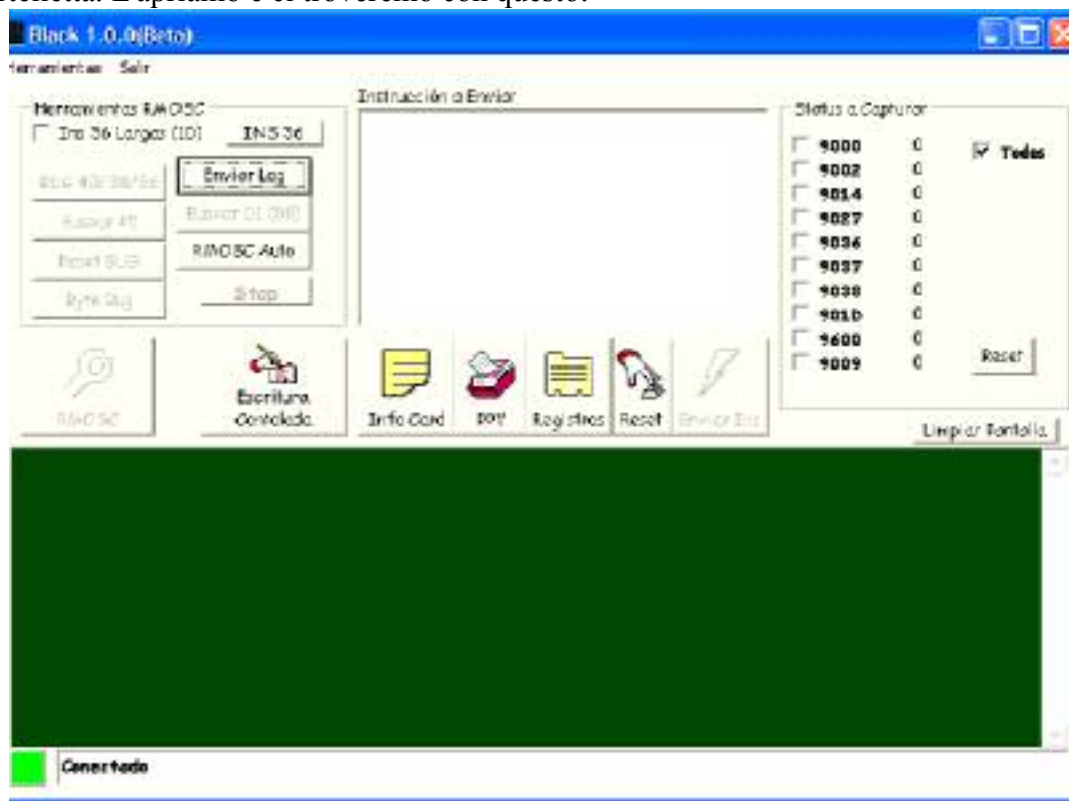
**Buono metámonos in lavoro manuale.** Diamo ovviamente che prima di affrontarvi al Black abbiamo già gli attrezzi necessari. Questo è:

Neretto in rango di aggiornamento.

Migliaia di istruzioni estratte per differenti vie.

Phoenix + xtal di 3'68. Per certo... è una pena che non fufe con uno di 6.

Una volta abbiamo il materiale necessario c'abbassiamo il Black e lo decomprimiamo in una cartelletta. L'apriamo e ci troveremo con questo:



Come vediamo il Black ha due parti fondamentali nei che lavorare:

RMOSC

Scrittura Controllata

Per difetto il programma c'è aperto nella prima... benché la maggior parte delle operazioni, ed i più interessanti, dovremo farli nella seconda. Che, inoltre, è quello che c'occupa.

Una volta che abbiamo avulso il programma con la card introdotta nel phoenix possiamo utilizzare i primi fattorini che abbiamo prima noi:



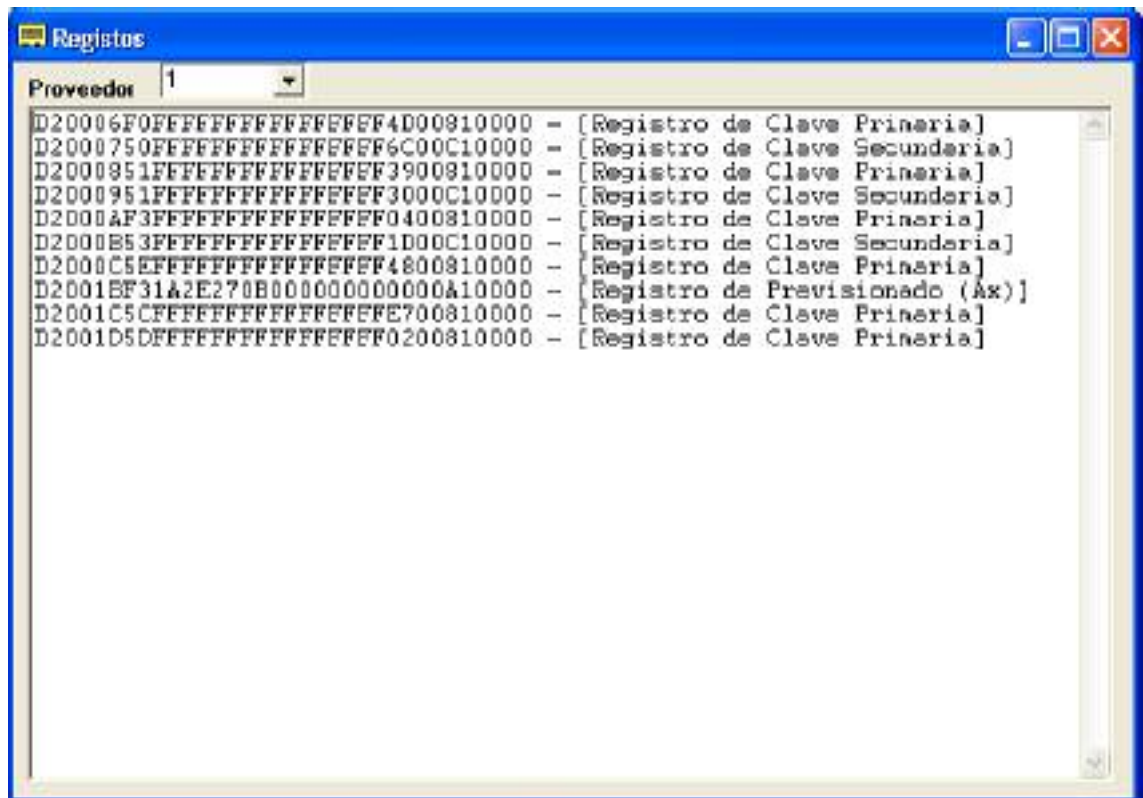
Con Info Card potremo leggere i dati del nostro biglietto che verrebbero ad essere questi:

The screenshot shows a window titled 'Información de la Tarjeta'. It has a 'Datos Generales' section with a 'Nº de Serie de la Tarjeta:' field. Below is a 'Proveedores' section with a table. The table has columns: 'Id del prov.', 'Nombre del Proveedor', 'PPUA', 'Fecha de Alta', 'PBM', and 'Key's Operativas'. There are four rows of data and one empty row at the bottom. A 'Actualizar Datos' button is at the bottom right.

Id del prov.	Nombre del Proveedor	PPUA	Fecha de Alta	PBM	Key's Operativas
0000	SECA	0000000	0/0/1990		F0
0064	CANALSATELITE	0001	31/7/2003	F1C050A478CF8CAD	F0 51 F3 5E 5C 5D
0066	CANALSATELITE2	001	31/12/2002	00000000000000	F0 F1 F3 FE
0067	CANALSATELITE3	001	31/12/2002	00000000000000	F0 F1 F3 FE

Evidentemente nell'esempio sono pubblicati i dati che potessero essere rivelatori come numero di serie del biglietto o le ppua's.

Con gli opzione Registros perché quello... potremo vedere i registri che abbiamo. Nell'esempio sarebbero i seguenti:

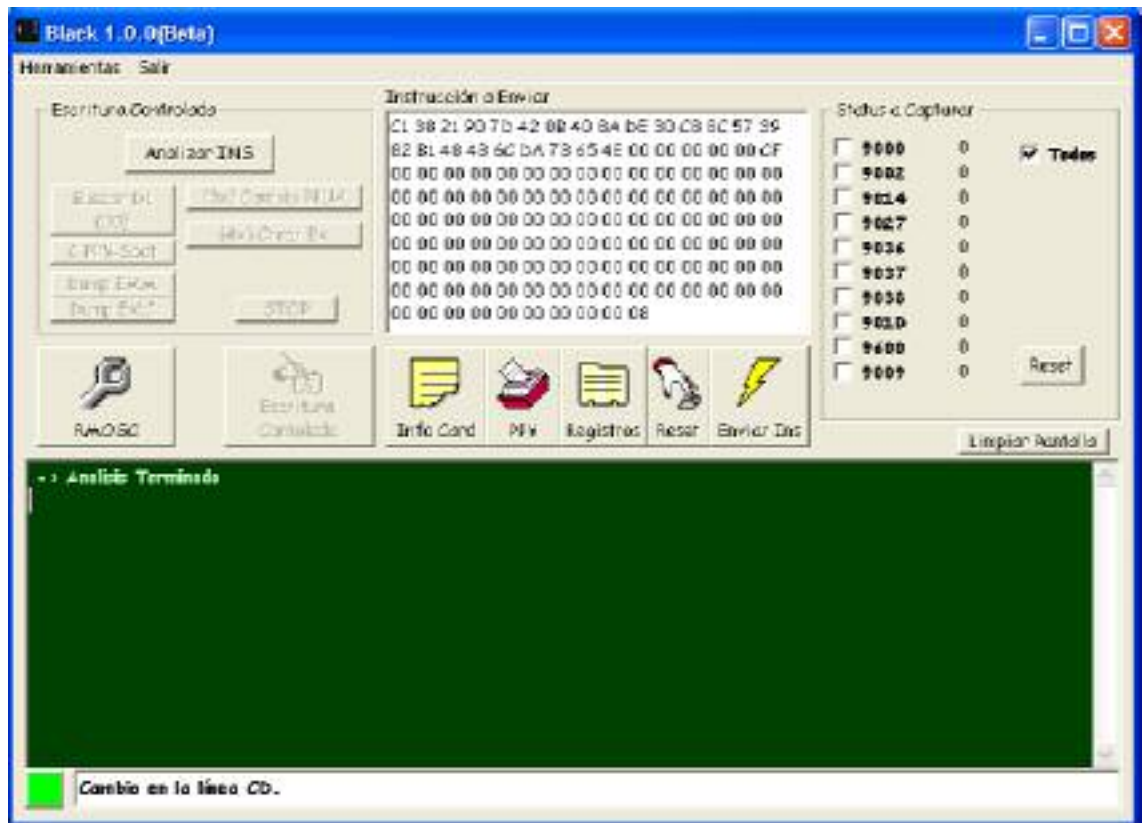


L'esempio ci viene ai capelli perché come possiamo comprovare il nostro card è orfana di registri Bx che sono quelli che necessitiamo. Perciò, prima di metterci in altre farine vediamo come possiamo fare per crearli rapidamente. **La prima raccomandazione è non passare creando registri... che dopo per quadrare il parsing diventeremo pecore.**

### Creazione di registri Bx

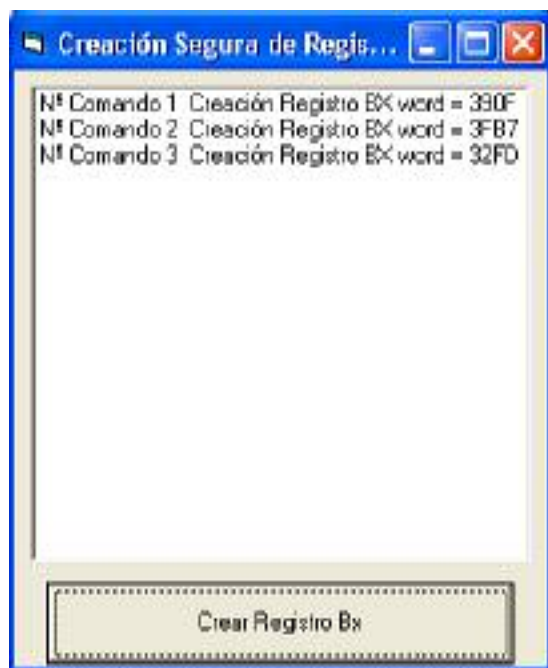
Tale e come dicevamo all'inizio è di supporre che c'impadronimmo già di un'importante provvista di c1 36 di tutti i colori cosicché ora quella che dobbiamo cercare è una del tipo 4x e convertirla a C1 38. Che come lo facciamo? Buono... io vi dirò come lo feci io. Tirai di un programma che si chiama Selfins e che si incarica di farlo direttamente. Per ciò la cosa unica che deve fare è collocare la c1 36 scelta nel casello corrispondente, selezionare Ins Testing, se questo è corretto si abiliterà l'opzione Pre Mount, ma prima di clicar in lei sceglieremo il LEN che io ho lasciato in 7D, e dopo sì che clicamos in Pre Mount. Una volta realizzata ci rimane solo clicar in Generati... et egli voila. La 38 sta intelligente e confezionata per portarcela al Black.

[illegible]



Una volta fatto questo il Black si metterà a lavorare, cosicché la cosa migliore sarà infiammarsi un'animo, prendere una birra... ed a rilassarsi.

Una volta che abbia fermato c'apparirà abilitata l'opzione di (4x) Creare Bx. Perché bene... a che cosa stiamo sperando? Facciamo clic e... voila:



C'appaiono i possibili registri Bx a creare. Il resto è facile. Fino allo seppi fare io. Solamente bisogna andare clicando di uno in uno fino a che ce li crede il Black.

Perché molto bene... abbiamo già i registri che tanto desiderava. Senza maggiori complicazioni ed in pochino tempo. Ma neanche crediamoci il latte... perché lo fece tutto il programma.

### Cambiamento di PBM

Una volta creati i registri vediamo se siamo capaci di mantenere l'integrità del nostro biglietto cambiandogli il PBM. Caricarci la sarà difficile per le agevolazioni che ci dà il Black... ma questo non sa della mia maestria nel momento di fabbricare bel sottobicchiere.

La cosa prima che dobbiamo fare è guardare i registri del nostro card. Per ciò clicamos nuovamente negli opzione Registri del Black e potremo vederli e, inoltre, nel formato che c'interessa:

D20006F0FFFFFFFFFFFFFFFFE00810000 - [Registro di Chiave Primaria]  
D2000750FFFFFFFFFFFFFFFFB800C10000 - [Registro di Chiave Secondaria]  
D2000851FFFFFFFFFFFFFFFFF0600810000 - [Registro di Chiave Primaria]  
D2000951FFFFFFFFFFFFFFFFF6200C10000 - [Registro di Chiave Secondaria]  
D2000AXXXXXXXXXXXXXXXXXXXE10000 - [Registro Sconosciuto]  
D2000B8E1B4C270A4E270B572701A10000 - [Registro di Previsionado (Ax)]  
D2000C5EFFFFFFFFFFFFFFFFF9600810000 - [Registro di Chiave Primaria]  
D2001B5CFFFFFFFFFFFFFFFFF8000810000 - [Registro di Chiave Primaria]  
D2001C5DFFFFFFFFFFFFFFFFF1000810000 - [Registro di Chiave Primaria]  
D2001D0079DDFFC80000FFFF0000B10000 - [Registro PPV (Bx)]  
D2001E006368FF1D0000FFFF0000B10000 - [Registro PPV (Bx)]  
D2001F009637FFB20000FFFF0000B10000 - [Registro PPV (Bx)]  
D20020008DC7FF9B0000FFFF0000B10000 - [Registro PPV (Bx)]  
D20021005074FFC80000FFFF0000B10000 - [Registro PPV (Bx)]

Bene. Una volta conosciuti cercherò tra le mie istruzioni una 7x che miri direttamente ad un registro di chiave della quale ho. Come lo faccio? Perché bene, zoppo l'Ultraedit ed apro lo schedario delle ins 7x. Li gli faccio cercare e gli dico che mi cerchi le seguenti catene: 82 00 0 e 82 00 1, quello che viene ad essere tutte le ins con D2=00 e D3 con 0x e 1x. Dopo alcuni secondi appariranno i risultati che io mi porto alla valigetta per studiare le possibilità che ho. Questo fu quello che mi diede l'Ultraedit:

C1 36 21 90 14 36 13 7E AB F3 15 40 77 7F 4D 07 D.C. 82 00 0E AB 2E 26 2A B3 EE  
C1 36 21 90 14 36 13 77 9B 09 11 20 BF 11 AC D5 0C 82 00 08 4E B4 71 D.C. 63 65  
C1 36 21 90 14 36 13 72 AB 7D A7 E0 61 42 90 D0 A0 82 00 06 C9 B2 AD 3A 7A 2F  
C1 36 21 90 14 36 13 7A 63 3D 10 7F 91 BD 63 A3 A0 82 00 09 14 76 CE 4A BD 4B  
C1 36 21 90 14 36 13 77 53 E8 DF 7D EE Fa 8C 0C 94 82 00 1B 5E 44 8C D.C. DD  
B0  
C1 36 21 90 14 36 13 73 F3 44 7A A8 F4 97 E1 87 F2 82 00 10 94 7A EE B4 81 D0  
C1 36 21 90 14 36 13 79 3B 88 85 35 BD 79 Fede 8F 31 82 00 19 15 66 2A 0E Dà 3B  
C1 36 21 90 14 36 13 78 1B D1 7A 9E C2 DB 7D C8 F5 82 00 1A 5F F2 F8 01 07 E4

Tale e come può apprezzarsi ho varie di esse che mirano direttamente ad una chiave. Che come lo so? Perché buono... facciamo l'esempio del quale utilizzo per vedere se sono capace che spiegarmi. Per tentare di ottenere un buon PBM prenderò questa:

C1 36 21 90 14 36 13 72 AB 7D A7 E0 61 42 90 D0 A0 82 00 06 C9 B2 AD 3A 7A 2F  
che mira direttamente al mio primo registro:

D20006F0FFFFFFFFFFFFFFFFFEE00810000 - [Registro di Chiave Primaria]

Molto bene, ho l'ins, ho il black... posso cambiare già il PBM. **Pos no.** Manca comprovare il parsing. Juerrrrrrrrr... e quello che è?? Perché è la cosa più importante del processo e che se fai male, avrai alcune possibilità abbastanza grasse di eseguire un nano malconcio e comandare tutto a prendere per sacco. E, come calcolo il parsnig dei miei registri? Buono cerco di spiegarlo nella pratica... ma non mi faccio responsabile di quello che possa passare.

## IL PARSING

Più su abbiamo visto i registri che aveva nel mio card. Di quello che si tratta ora è calcolare che nanos esegue mentre dumpeo per ottenere il cambiamento di PBM, e che quelli nanos non sia malconcio. Per ciò partiremo dell'idea che andiamo a dumpar sei registri dall'eletto. Siete già conoscitori, suppongo, che un byte è ognuna dei compagni che si comporsi un'ins ed il primo valore di ogni byte è chi c'indicherà il numero di salti a realizzare seguendo la seguente tavola:

Byti Salti

0x 0

1x 1

2x 2

3x 3

4x 4

5x 5

6x 6

7x 7

8x 8

9x 9

Ax 10

Bx 11

Cx 12

Dx 16

Ex 24

Fx 32

Ben ora prendiamo il primo registro dei miei:

D20006F0FFFFFFFFFFFFFFFFFEE00810000

Come il nano che eseguiamo per il cambiamento del PBM è il 80 dovremo incominciare dando un salto 8 byti dal primi:

D20006F0FFFFFFFFF

FF \*

FFFFFFEE00810000

Come vediamo questo salto ci porta fino ad un compagno di FF che c'obbliga ad un salto di 32 byti... e così via. L'obiettivo è arrivare fino al fine dei registri a rovesciare senza cadere in nanos maliziosi e cadere alla fine di tutto in 03 o 82 che è quello che dovremo mettere alla fine del nostro ultimo registro. Se per il mezzo cadessi in un D2 l'avrai succhiato perché ti porterà direttamente alla linea di meta. Tieni in conto che ogni registro sono 17 byti e come vedemmo nella tavola Dx=16 salti. Prima di vedere il caso pratico saprai che quando faccia un salto sarà il seguente byte dell'ultimo quello che ti indicherà il nuovo valore del salto e che quello non conterà per farlo. Tieni anche in conto che se cadessi in un 00 andrai fino al seguente per sapere il numero di salti di realizzare. Vestisti già che 0x=0 salti.

Vediamolo nella pratica. Rimanessimo che andava ad utilizzare il primo registro e che andava a fare un rovesciato di 6 con quello che utilizzerebbe i seguenti:

```
D20006F0FFFFFFFFFFFFFFFFFEE00810000
D2000750FFFFFFFFFFFFFFFFFB800C10000
D2000851FFFFFFFFFFFFFFFFF0600810000
D2000951FFFFFFFFFFFFFFFFF6200C10000
D2000A5030C34644344D724C3B45E10000
D2000B8E1B4C270A4E270B572701A10000
```

Perché il parsing di questi registri farebbe bella figura così:

```
80
D2 00 06 F0 FF FF FF FF
FF *
FF FF FF EE 00 81 00 00 D2 00
07 50 FF FF FF FF FF FF FF FF
B8 00 C1 00 00 D2 00 08 51 FF
FF FF
FF *
FF FF FF FF 06 00 81 00 00 D2
00 09 51 FF FF FF FF FF FF FF
FF 62 00 C1 00 00 D2 00 0A 50
30 C3
46*
44 34 4D 72
4C *
3B 45 E1 00
00 D2 *
00 0B 8E 1B 4C 27 0A 4E 27 0B
57 27 01 A1 00 00
```

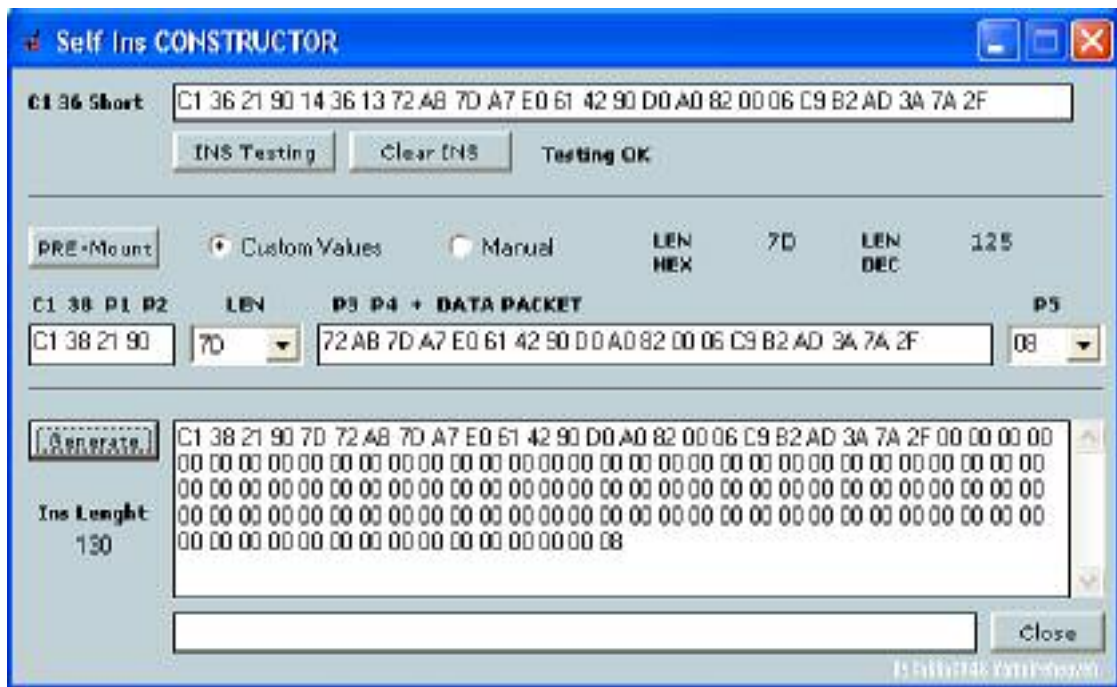
03\* 82

Tale e come posso comprovare non cado in nessun nano malizioso, sono marcati con asterisco, ed alla fine vado diretto ad un D2 che mi porta fino al 03 fine..... BINGO.

Suppongo che non vi sarà rimasti molto chiaro il tema del parsing... ma sicuro che vi aiuteranno gustosamente a capirlo genti di più sapere che io.



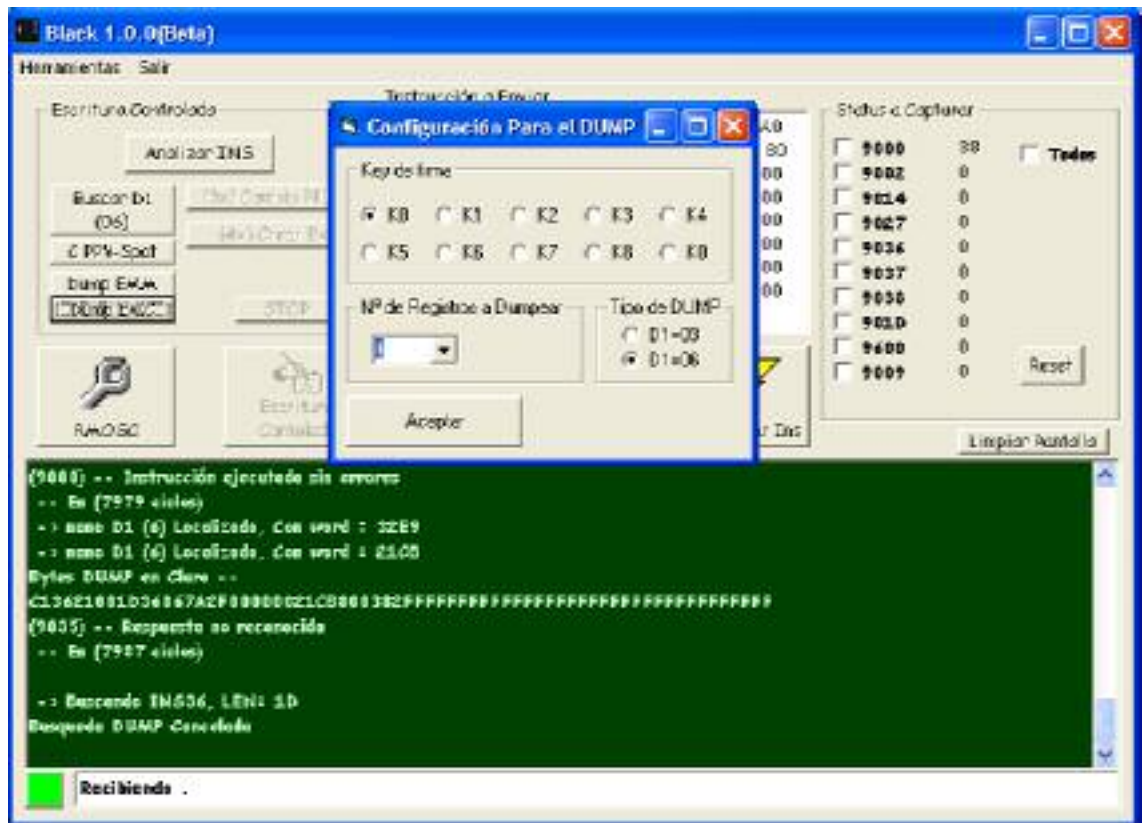
Il caso è che ho già i miei registri creati, benché alla fine non avessi bisogno di essi per il PBM perché ebbi la fortuna di trovare una meraviglioso ins 7x con D2 D3 = 00 06. Ho anche l'ins che necessito per dumper e che mira ad una key e ho il black. Che cosa devo fare ora? Perché la stessa cosa che per creare registri... cambiare l'ins 36 a 38, e per farlo torniamo ad utilizzare il Selfins e realizziamo ma lo stesso processo di prima in questa occasione collochiamo la 7x selezionata e la trasformamos affinché ci rimanga della seguente maniera:



Ora prendo la c1 38 e faccio l'attenzione a cambiargli il sesto byte post firma che è un 00, per 80. Una volta fatto questo apro nuovamente il nostro meraviglioso Black e clico in Scrittura Controllata. Una volta attacco lì l'ins nel suo posto. Una volta fatto questo vado alla Herramientas/Configuración Avanzada e seleziono la SSE del mio card della seguente forma:



Accetto e solamente mi rimane fargli Analizzare Ins. Una volta che il programma si ferma abiliterà l'opzione di Dump Emm. Clicamos su lei e c'apparirà un'altra ventan nella quale ci saranno chiesti i parametri corretti per realizzare il Dump. Perché bene, tale e come si mostra nell'immagine, io ho utilizzate la k0 per la firma col tipo D1=06 e con 6 registri a dumpear.



Una volta fatto accettato comincia la ricerca. In questo punto bisogna lasciare tranquillo al Black. Il processo, in ogni modo, non dovrebbe trattenersi molto.

Una volta finito il Dump il proprio Black c'avvisa con la seguente leggenda alla fine della finestra:

Risposta valida contraria!  
Ricerca DUMP finito

Giusto sopra a questi messaggi potremo vedere una 61 38 che utilizzeremo per il cambiamento del PBM, ma prima vediamo come c'apparirebbe nel programma:



Ora andiamo al Mosaic e gliela comandiamo ed aspettiamo la risposta.... **90 00**. Se ce la dà ci rimane solo cambiare il 38 con un 40 e comandargli la C1 40 e pregare affinché non abbiamo messo la zampa in qualcosa.

Finalmente il Mosaic si divora l'ins... e ci cambia il PBM. Questo servitore aveva così prima la card della seguente forma:

Provider PID PPUA PBM Dati

```
|00 | secca |0000 | |00000000 | |0000000000000000 | 00.00.1990
|01 | CANALSATÉLITE |0064 | |0D..... | | D2001B5CFFFFFFFF | 31.01.2004
|02 | CANALSATÉLITE2 |0066 | |0B..... | |0000000000000000 | 31.12.2002
|03 | CANALSATÉLITE3 |0067 | |0B..... | |0000000000000000 | 31.12.2002
```

Ed ora mi è rimasto così:

Provider PID PPUA PBM Dati

```
|00 | secca |0000 | |00000000 | |0000000000000000 | 00.00.1990
|01 | CANALSATÉLITE |0064 | |0D..... | | D20006F0FFFFFFFF | 31.01.2004
|02 | CANALSATÉLITE2 |0066 | |0B..... | |0000000000000000 | 31.12.2002
|03 | CANALSATÉLITE3 |0067 | |0B..... | |0000000000000000 | 31.12.2002
```

Come potete comprovare il mio nuovo PBM, D20006F0FFFFFFFF, coincide col registro utilizzate per dumpcar:

D20006F0FFFFFFFFFFFFFFFFFEE00810000 - [Registro di Chiave Primaria]

Ed inoltre ha le sufficienti FFFFF affinché sia un PBM full\_quetecagas.

Buono... perché queste sono le mie esperienze col Black. Un stupendo programma che ci permette ad autentici dritti come io intrattenerci un momento senza correre troppi rischi. Se continuasse a disordinare con lui... vi seguirò già contando le mie esperienze.

Un saluto... e congratulazioni un'altra volta ai desarrolladores/betatester's del Black.