

INFORMAZIONE LIBERA CREW
E-zine 04

www.informazione libera.cjb.net ~ cyberdude1L@libero.it



PRESENTA:
OpenSky Resolution
LAVORO DI : UNRELATED TAILOR E MYSTIC

QUESTO TESTO E' STATO TROVATO e modificato IN RETE DA TAIL** e L.Unre*****L. il merito è di mystic

Data: 05/09/2003

Come molti di voi ormai ben sapranno e come già ho avuto modo di spiegare in altre mie guide sulla tv satellitare (siete dei miei fans ormai vero?), con l'introduzione da parte delle aziende di streaming satellitare dell'estensione della codifica Seca chiamata Seca2, gli antichi metodi che i sat-hackers usavano per guardare a sbafo le trasmissioni sono stati resi inutili. Wafer, PicCard e Fun sono state completamente oscurate da un semplice aggiornamento della codifica con il quale venivano e vengono tutt'ora crittate le trasmissioni televisive satellitari. L'innovazione sta nell'utilizzo dell'Envelope (Secondary Super-Encryption), che si comporta come una seconda chiave di crittatura che lavora in parallelo alla Primary Super-Encryption che già funzionava ai tempi del vecchio Seca. Ma basta teoria, passiamo alla pratica. Sò che a molti di voi non interessa assolutamente di conoscere come funzionano le cose e me ne dispiaccio, ma sono buono e voglio favorirvi ;)

Prima di tutto cos'è questa V7 di cui tanto sentite parlare? E' semplicemente una smartcard di colore bianco (ecco perché alcuni la chiamano "bianchina") in tutto e per tutto simile alle vecchie smartcard nere di D+, ma con implementate le nuove funzioni di Envelope di cui poco più sopra vi parlavo. Come ogni nuova tecnologia, al momento della sua nascita non è mai perfetta. Grazie al lavoro di alcuni ragazzi spagnoli e italiani si è giunti alla conoscenza di un bug nei comandi inviati dal provider TELE+ DIGITALE per l'aggiornamento mensile delle chiavi di visione. Come già probabilmente avrete avuto modo di scoprire leggendo altre guide tra cui l'ottima "Capire gli ECM/EMM", il bug 36/38 è proprio quello che sfrutteremo per ottenere il pieno controllo della nostra carta pur non essendo in possesso delle chiavi operative con cui firmare i comandi da inviarle.

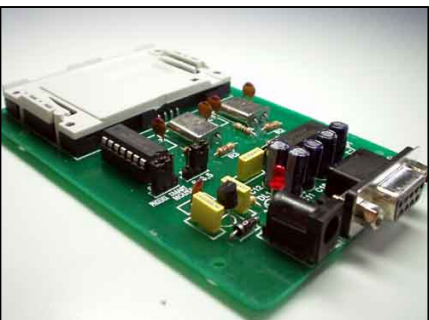


Prima di gioire convinti di poter vedere stasera stessa la vostra serie preferita su Fox o la vostra partitella del cuore su Sky Sport 1, vi faccio un brevissimo elenco di cosa ci potrebbe essere utile all'operazione di analisi e modifica del contenuto della smartcard. Sarà sicuramente necessario uno SmartMouse a 3.57/6 Mhz. Meglio a 6 Mhz, così le operazioni verranno svolte più velocemente. Necessaria sarà anche una INS C140 di aggiornamento ricavata da un log di dicembre 2002 o gennaio 2003; molti ora mi chiederanno perché proprio di questi due mesi. Semplicissimo: perché alla fine di gennaio TELE+ DIGITALE si è accorta del madornale bug presente sui log di aggiornamento in corso di trasmissione e ha tentato di correggere il danno ormai fatto. Ci sarà utilissima anche una INS C140 di aggiornamento del mese corrente, in quanto ci permetterà di aggiornare la nostra smartcard ai diritti di visione attuali senza dover inserirla nel decoder ed attendere un aggiornamento da parte di TELE+ DIGITALE.

I Software necessari per l'analisi e la scrittura della nostra V7 sono rispettivamente MKFind 4.4 o superiori e il mitico UCDS 4.9 Gold (anche l'ultimissimo 5.01 o i successivi vanno benissimo), nel quale il mitico goldfinger ha messo tutto il suo impegno riuscendolo a rendere un programma efficace ma allo stesso tempo alla portata dei meno esperti.

Per evitare di far perder tempo a chi non ne ha dico subito che potrà lavorare sulla propria bianchina con una elevata possibilità di successo solo chi ha eseguito l'attivazione della stessa in data antecedente all' 1 Febbraio 2003. Volete sapere il perché? Non voglio dilungarmi ma tento di farvi capire brevemente: partendo dal presupposto che ogni mese TELE+ DIGITALE invia ai propri sottoscrittori gli aggiornamenti (le vecchie INS C140), bisogna sapere che questi vengono inviate unicamente verso le schede attive. Se una scheda quindi non è stata attivata entro il 1 Febbraio 2003 avrà possibilità praticamente nulle di trovare una INS C140 di aggiornamento di Dicembre 2002 o Gennaio 2003 atta a sfruttare il bug 36/38; non gli rimarrà quindi che abbonarsi a Sky Italia e mettersi il cuore in pace. Avete capito tutto ragazzi? Siete pronti a partire? ;)

ANALIZZIAMO LA V7:



Inseriamo la scheda nello SmartMouse impostato a 3,57 Mhz ed apriamo il software MkFind 4.4. Una volta connesso il programma lavorerà per qualche secondo fino a mostrare molti dati utili. Vedremo subito una lista dei provider attivi sulla V7, tra cui TELE+ DIGITALE. Per rendervi ancora più facile l'analisi io vi consiglio di operare immediatamente un salvataggio dei dati ricavati su file: potrete fare questa operazione accedendo al menu File – Save File e selezionando

l'opzione "Save MKF Key File". Ovviamente se selezionate la lingua italiana i messaggi ottenuti saranno lievemente diversi, ma siccome avete un cervello penso che sarete in grado di salvare il vostro file MKF. Una volta effettuata questa operazione chiudiamo pure MkFind 4.4 e andiamo ad analizzare con un banale editor di testi quale notepad il file MKF salvato un attimo fa. Noteremo una schermata simile a questa:

```
[General Info]
ATR= 3b f7 11 00 01 40 96 70 70 07 0e 6c b6 d6
UAhex= ?? ?? ?? ??
UAdec= ????.???.???
SuppProv= 00000000000011111

[00 00]
Name= SECA
SECASStartup= 00 00 00 00 00 00 00 00 00 80
SECAPPV= ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
PrimaryKeys= f0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

[00 70]
Name= TELE+ DIGITALE
Date= 31/08/2003
PPUA= ?? ?? ?? ??
Region= 00
PBM= ?? ?? ?? ?? ?? ?? ?? ??
PrimaryKeys= f0 51 5c 5d 5e ff ff ff ff ff ff ff ff ff ff ff ff

[00 71]
Name= +CALCIO
Date= 00/00/1990
PPUA= 00 00 00 00
Region= 00
PBM= 00 00 00 00 00 00 00 00
PrimaryKeys= f0 f2 f3 ff ff ff ff ff ff ff ff ff ff ff ff ff

[00 72]
Name= OPERATORE 1
Date= 00/00/1990
PPUA= 00 00 00 00
Region= 00
PBM= 00 00 00 00 00 00 00 00
PrimaryKeys= f0 f2 f3 ff ff ff ff ff ff ff ff ff ff ff ff ff

[00 73]
Name= OPERATORE 2
Date= 00/00/1990
PPUA= 00 00 00 00
Region= 00
PBM= 00 00 00 00 00 00 00 00
PrimaryKeys= f0 f2 f3 ff ff ff ff ff ff ff ff ff ff ff ff ff
```

Notiamo subito che l'unico provider che sembra essere attivo (la data è la più aggiornata, e se guardate le PrimaryKeys trovate le indispensabili f0 e 51) è 00 70, ovvero TELE+ DIGITALE. Vi dico fin da subito che se non avete la chiave f0 ma soprattutto la chiave 51 nel provider che volete andare a modificare partite male, in quanto non vi sarà assolutamente possibile far scattare il bug 36/38 sulla V7 senza prima aver tentato la riattivazione del provider tramite apposito log di attivazione. Il log di attivazione dovrà venire cercato in base alla vostra UA in formato esadecimale (la trovate nel file MKF sotto la dicitura UAhex). Con questa alla mano provate su #informazioneelibera a controllare se sul fserv del canale è presente qualche attivazione che fa al caso vostro. Ricordate che l'attivazione è da cercarsi del mese solare in cui la vostra carta è stata attivata! Mi spiego meglio: se avete attivato la vostra scheda nel lontano ottobre 2002, dovrete cercare un log di attivazione di ottobre 2002 in quanto probabilmente sarà l'unico in cui il vostro UA comparirà in tutto il suo splendore e l'unico quindi da cui estrapolare con sicurezza la INS di attivazione per il provider senza chiavi operative. Se non siete sicuri su questo passo potete sempre domandare aiuto su # informazioneelibera

Supponiamo quindi di voler modificare i dati del provider 00 70 e di avere le necessarie f0 e 51. Prima di tutto cosa davvero si può modificare sulla nostra bianchina? Girano così tante voci fasulle per la rete che quasi sicuramente sarete tutti un po' spaesati e sarebbe ora di fare un po' di chiarezza. Le cose modificabili tramite il Bug 36/38 sono virtualmente infinite, ma le operazioni che si possono fare con una relativa facilità, rapidità e una probabilità di danneggiare la carta relativamente ridotta sono tre:

Cambio PPUA: Necessario qualora la vostra carta sia scaduta (non si aggiorni più mensilmente). L'operazione viene fatta in modo automatico dall'ottimo UCDS 4.9 Gold e consiste nel tentare il continuo cambio di SA e CWP fino a che non venga trovato un CWP attivo che risponda positivamente alla INS C140 di aggiornamento del mese corrente. L'aggiornamento viene effettuato quindi istantaneamente appena trovato un PPUA "buono" e la data di fine diritti schizza all'ultimo giorno del mese successivo a quello in cui viene loggata la INS C140 di aggiornamento.

Cambio Data: I più attenti si chiederanno perché mai cambiare data. Infatti vi ho appena detto che una volta trovato un CWP attivo la carta viene automaticamente aggiornata dalla stessa INS C140 e la data viene modificata. Anche se tentassimo di spingere la data in alto non avremmo comunque le chiavi operative aggiornate alla visione degli eventi, quindi non vedremmo nulla. E allora perché cambiar data? Ve lo spiego subito. Mettiamo caso che i vostri diritti di visione siano scaduti a Marzo 2003. Ora volete ripristinare la V7, ma... ops.. stranamente seppur cambiando CWP ne trovate uno attivo la bianchina non prende l'aggiornamento! Ecco il perché: gli aggiornamenti delle chiavi operative possono avvenire al massimo ogni bimestre! Se avete quindi i diritti scaduti da Marzo non potrete inviare nessun aggiornamento valido per una data superiore a Marzo + 2 mesi = Maggio. Come fare allora a scavalcare il problema? Semplicissimo, basta far schizzare in avanti la data! In questo modo riusciremo a mandare in confusione il sistema di protezione della V7 che accetterà anche aggiornamenti più recenti.

Cambio PBM: Il PBM è una matrice di byte (o meglio un vettore, per i puristi dell'algebra) che immagazzina al suo interno informazioni riguardo ai canali a cui siamo abilitati in visione. Grazie a questo ogni volta che vi posizionate su un canale digitale satellitare viene effettuato un controllo del vostro PBM. Se il byte controllato è superiore a una certa soglia sarete abilitati alla visione, se no vedrete solo uno schermo nero! Grazie al bug 36/38 è possibile modificare aleatoriamente anche questa matrice di byte per rendere possibile la visione di un numero molto più elevato di canali appartenenti al pacchetto Sky.

Mi sembra di avervi detto tutto, quindi ormai vi sarete fatti un'idea di cosa vi serve. Naturalmente per chiunque avesse il PBM pari a 00 00 00 00 00 00 00 00 (è una tecnica che usa TELE+ DIGITALE per impedire la visione a chi avesse l'abbonamento scaduto), dovrà prima aggiornare il proprio CWP e conseguire l'aggiornamento delle chiavi operative e una volta fatto questo potrà procedere al cambio di PBM abilitando il provider alla visione dei canali che altrimenti con un PBM azzerato non potrebbe vedere. E ora ecco ciò che i più frettolosi di voi tanto aspettavano (ma che parlo a fare, tanto di sicuro avranno saltato questa parte informativa ;P).

IMPORTANTE: Salvate e tenete con cura da qualche parte il file MKF, vi sarà utilissimo anche in futuro per ulteriori referenze o ulteriori cambi! Mi raccomando: se decidete di non seguire il mio consiglio poi non venite a piangere su # informazionelibera!!! Vi riderò in faccia con gusto!

RICAVARE LE INS C140 DAI LOG:

Ecco una parte che sarà sicuramente utilissima a molti di voi. Non immaginate nemmeno quante persone mi contattano ogni giorno chiedendo come ricavare la INSC140 da un log precam. E' un'operazione che al neofita spesso risulta più complicata di quanto non lo sia e ora ve lo dimostrerò:

Mettiamo caso che la vostra SA sia 09CB0D. Come potrete ben notare la SA è composta dai primi tre byte del PPUA, ed è proprio questa che dovremo cercare nei log. Apriamo il nostro file che contiene le INS C140 di aggiornamento. Naturalmente se è un file testuale useremo notepad, se invece è un file in formato binario useremo un editor binario esadecimale quale WinHex. Inserendo come chiave di ricerca la nostra SA ci apparirà una sfilza di dati simile:

09CB0D00B11001108FE7B83DAEBADE1D81757346661073D7C6F36D77153C62DDD9081C3D684BF82
03A0DA03EEB7D79BF3442CD4BD871BE907D9A7FB41B1EBAAEF3A6B4242B1F975B4BE4E98A8AFA7F
2C4C04CA4EE03F0824C39D4847412619066CB806897897840063.....

Ho già provveduto ad evidenziarvi le parti più interessanti della stringa esadecimale in modo che vi sia più facile capire ciò che starò per dirvi. Prima di tutto vedete all'inizio del log la SA 09CB0D. Vi accorgete che state guardando un log valido in quanto subito dopo noterete i byte: 1001. A questo punto tutti i byte fino alla stringa 840063 faranno parte della nostra INS. Questi ultimi byte sono utili solamente a separare una INS da un'altra durante il trasferimento dati da parte di TELE+ DIGITALE.

Ora seguendo le mie indicazioni avrete in mano una stringa esadecimale così composta:

1001108FE7B83DAEBADE1D81757346661073D7C6F36D77153C62DDD9081C3D684BF8203A0DA03EE
B7D79BF3442CD4BD871BE907D9A7FB41B1EBAAEF3A6B4242B1F975B4BE4E98A8AFA7F2C4C04CA4E
E03F0824C39D4847412619066CB806897897

Mi chiederete ora: perché hai evidenziato in blu anche quei 5 bytes? Semplicissimo. Quando notate nella vostra INS questi tre bytes "474126" dovete eliminarli, eliminando anche i due bytes a seguire. Non mi dilungo in spiegazioni teoriche sul perché di questa operazione per non appesantire ulteriormente il trattato. Quindi in questo caso andremo ad eliminare 4741261906 ricavando una stringa di caratteri ora accorciata:

1001108FE7B83DAEBADE1D81757346661073D7C6F36D77153C62DDD9081C3D684BF8203A0DA03EE
B7D79BF3442CD4BD871BE907D9A7FB41B1EBAAEF3A6B4242B1F975B4BE4E98A8AFA7F2C4C04CA4E
E03F0824C39D486CB806897897

Cosa ci manca ancora?! Semplicemente il comando di aggiornamento da inviare alla smartcard! Basta aggiungere prima della stringa ricavata questi bytes: C14001B15C

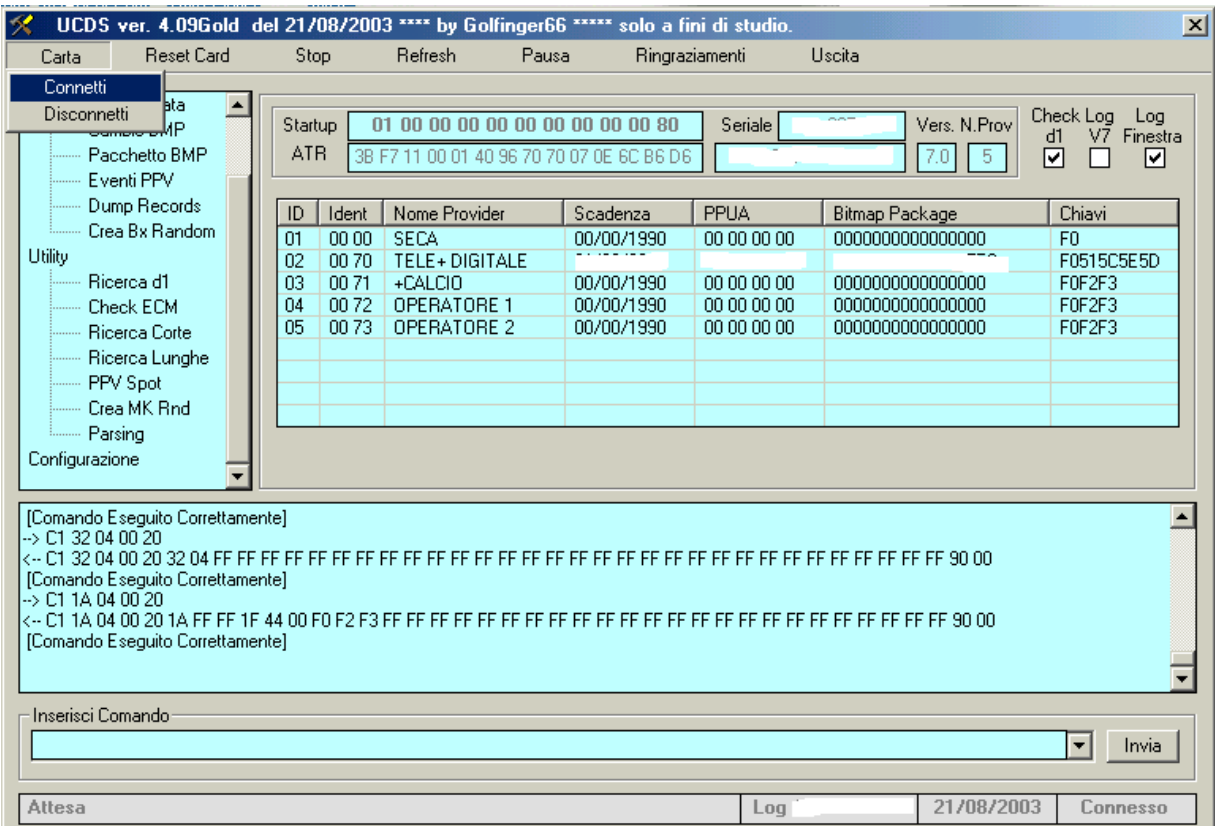
Il risultato finale sarà quindi il seguente:

C14001B15C1001108FE7B83DAEBADE1D81757346661073D7C6F36D77153C62DDD9081C3D684BF82
03A0DA03EEB7D79BF3442CD4BD871BE907D9A7FB41B1EBAAEF3A6B4242B1F975B4BE4E98A8AFA7F
2C4C04CA4EE03F0824C39D486CB806897897

Facile vero? Quando ci prenderete la mano sarà sicuramente più veloce che usare quegli scomodissimi programmi automatizzati che vi suddividono i log. E poi volete mettere la soddisfazione di ricavarvi la INS C140 con le vostre mani?

CAMBIO DEL PPUA E DELLA DATA:

Apriamo il programma UCDS Gold 4.09 e inseriamo la carta nello SmartMouse settato a 6 Mhz. Ricordo che UCDS andrà settato opportunamente per riconoscere uno SmartMouse a 6 Mhz, ma una volta riconosciuto le operazioni avverranno in modo notevolmente più veloce che a 3,57 Mhz. Clickiamo su CONNETTI e se tutto va bene la smartcard verrà letta e i dati relativi ad essa verranno mostrati nella finestra del programma. Ora possiamo anche chiudere UCDS. Quello che ci interessava è che il programma riconoscesse lo SmartMouse e la nostra bianchina e che creasse all'interno della directory in cui è stato installato una sottodirectory chiamata UAaabbccdd dove aabbccdd sono gli ultimi bytes della nostra UA (l'abbiamo letta poco fa in MKF, ricordate?). Entriamo ora in questa diretory e scegliamo il provider che vogliamo modificare. All'interno dell'archivio troveremo un sacco di file di



testo, molti dei quali vuoti perché aspettano di essere riempiti da UCDS o da noi stessi. Noi andremo ad aggiungere giusto un paio di cosette, poi torneremo al lavoro.

Apriamo il file Ins40.txt e qui aggiungiamo la INS C140 di Dicembre 2002/Gennaio 2003 necessaria a far scattare il fatidico bug 36/38. La stringa dovrà

essere aggiunta interamente e senza inserire spazi tra i vari bytes di cui è composta. Chiudiamo e salviamo il file, e apriamo ora il file InsAggiornamento.txt dove andremo a mettere la INS C140 del mese corrente. Questa ci servirà per far capire al programma quando avremo trovato un CWP attivo. Vi rammento che durante il cambio di PPUA qualora venisse trovato un CWP attivo l'aggiornamento avrebbe successo, la data verrebbe aggiornata così come le chiavi operative e il programma accorgendosi di interromperebbe l'operazione indicando AGGIORNAMENTO EFFETTUATO.

Una volta modificati i due file di testo possiamo riaprire il programma e connetterlo alla smartcard. Clickiamo ora su "Bug 36/38", la prima voce dall'alto nel menu. Se tutto va come dovrebbe entro 30 secondi UCDS dovrebbe indicarci quante C136 è stato in grado di estrapolare sfruttando il bug. Se non vengono trovate C136 consiglio di cercare una diversa INS C140 di Dicembre 2002/Gennaio 2003 e ritentare il bug.

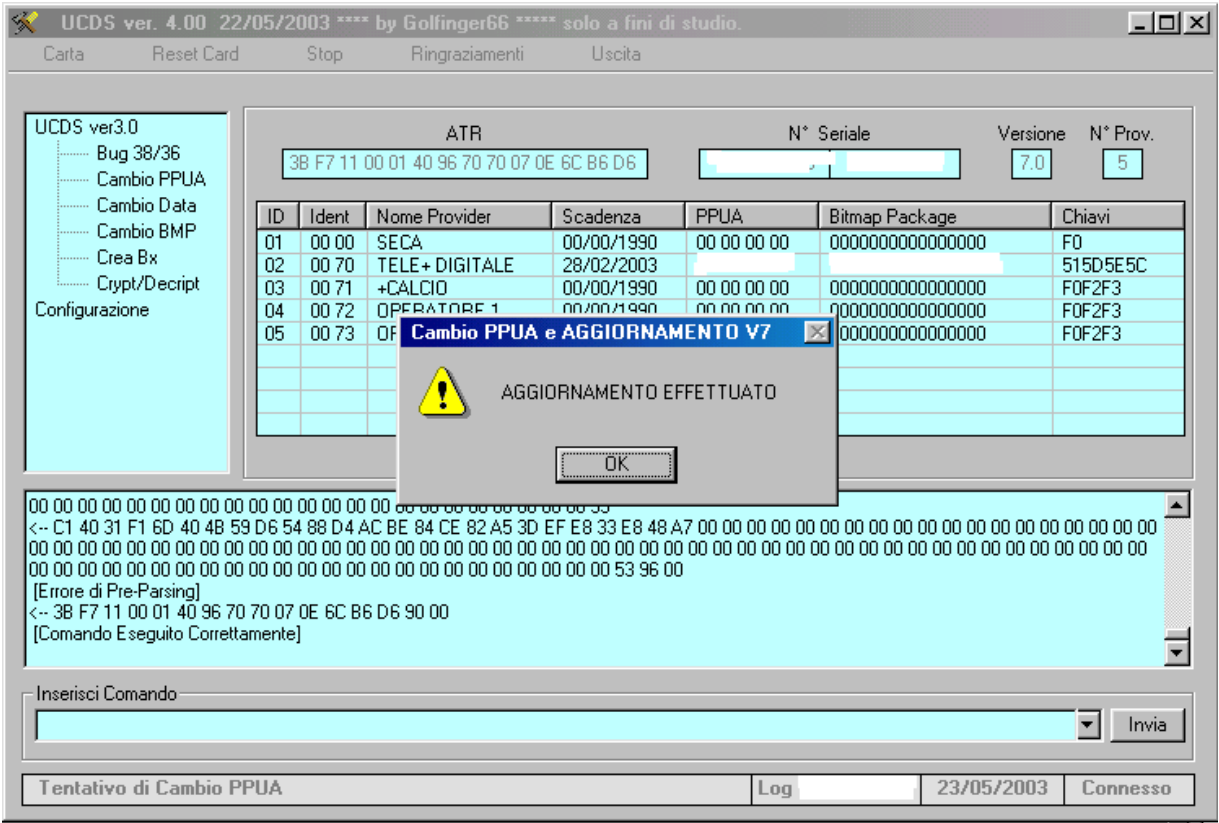
Apparirà appena avrete premuto su OK una finestrella indicante le tipologie di ricerche da compiere prima di procedere con i cambi di PPUA e di Data. Se dovete solo cambiare CWP e la data è a posto vi consiglio di impostare una ricerca per le sole chiavi P3 4x inserendo 10 o 25 nel campo di fianco a 4x. Se invece dovete cambiare anche la data selezionate anche il numero 5 o 10 nel campo P3 6x. Avviata la ricerca potreste dover attendere a lungo, dall'ora di tempo in su. Se vedete che il programma non trova nulla per parecchie ore sicuramente qualcosa non ha funzionato e vi consiglio di cambiare log C140 di Dicembre 2002/Gennaio 2003.

Appena la ricerca verrà portata a termine procedete ai vari cambi. Se la vostra data necessita di una aggiustata prima di procedere all'aggiornamento del CWP vi consiglio di farla ora. Clickate quindi su Cambio Data e attendete pazientemente. Entro breve (meno di 15 minuti solitamente) la vostra data verrà modificata. Se la data ricavata sarà superiore a quella dell'aggiornamento da effettuare non ci saranno problemi. Spesso risulteranno date altissime e spropositate (es. 2050). Vanno benissimo! L'importante è che non vi compaia una data più bassa di quella dell'aggiornamento! Se così fosse dovrete nuovamente procedere ad un cambio della data clickando su Cambio Data.

Ora è il momento di procedere al cambio della PPUA. Clickate sull'apposita sezione e ben presto il programma frullerà in ricerca di un nuovo CWP. Potrete vedere parecchi tentativi di cambio prima di ottenere un aggiornamento vero e proprio. Perché questo? Ve lo spiego subito: come ho tentato di farvi capire prima la INS C140 di aggiornamento per il mese successivo viene inviata da TELE+ DIGITALE mensilmente solo alle card effettivamente

attive. Se la vostra carta è disattivata il vostro CWP originale non sarà più registrato e quindi l'aggiornamento inviato mensilmente non lo comprenderà. Cosa c'entra questo con noi? Semplicemente UCDS tenterà più volte il cambio di CWP e se per puro caso indovinerà un CWP attivo l'aggiornamento mensile verrà effettuato con successo e il messaggio risultante sarà quello che potete vedere in questa gioiosa figura più in alto. Chissà quanti di voi aspetteranno impazientemente di leggere questo messaggio durante il cambio di PPUA...

Quando l'aggiornamento sarà effettuato siete teoricamente abilitati alla visione. Se inserite la bianchina nel decoder e vedete ancora buio probabilmente è perché il vostro PBM è azzerato. Che dite di cambiarlo assieme?



Clickate senza pensarci su Cambio PBM. Probabilmente il programma vi annuncerà che siete pazzi se sperate di poter cambiare il PBM senza prima aver trovato delle P3 7x corte. Accontentiamolo allora!

cliccando su Uscita. Fatto questo UCDS avrà le P3 7x corte per ricercare la C136 lunga necessaria all'operazione di cambio PBM. Clickiamo quindi su Cambio PBM e il programma si metterà al lavoro. Entro una mezz'ora l'operazione di ricerca delle C136 lunghe dovrebbe essere giunta al termine e dovrebbe iniziare l'operazione vera e propria di tentativo di cambio del PBM. Questa risulterà sicuramente lunghissima e vi consiglio quindi di farla di notte o di uscire a farvi un lungo giro ;) Nel mio caso sono state necessarie 13 ore di lavorazione.

CONSIDERAZIONI E CONSIGLI:

programma di riconoscere l'abilitazione della smartcard ai pacchetti offerti da Sky. La funzione per ora risulta particolarmente scarna e imprecisa, ma è da apprezzarsi particolarmente l'impegno messo dall'autore nella sua realizzazione.

E così ora avete la vostra nuova V7 abilitata alla visione di Sky. Non siete contenti? ;) Spero che questo documento sia stato utile a tutti coloro che fino a poco fa non capivano nulla di quello che si poteva fare e di quello che invece era solo una stupida invenzione di qualche amico saccente. Questo è quanto sappiamo (o ciò che vogliamo farvi sapere ;P) noi della # informazionelibera Crew ad oggi, ma ben presto vi stupiremo con altre importanti novità!

IMPORTANTE: Ora che avete apportato importanti modifiche alla smartcard vi consiglio di usare il blocker di fox007 per proteggerla da eventuali reset inviati via satellite da Sky. E' essenziale! Mi raccomando di non inserire la V7 senza un blocker fox007 v4.1B dotato di microcontrollore pic 16f628 nel decoder! In caso contrario la probabilità di ritrovarsi presto al buio è altissima! Per la configurazione del blocker vi rimando ad una delle guide scritte da me: "Il Blocker di fox007, questo sconosciuto

RINGRAZIAMENTI:

E' ormai venuto il momento di salutarci! Vorrei ringraziare per la collaborazione tutti i miei amici della #informazionelibera Crew, sperando prestissimo di farmi rivedere sul panorama satellitare con una nuova guida tutta per voi! Sono convinto che ben presto avremo novità rilevanti, ci resta solo da aspettare per.... vedere! ;)

Auguri a tutti! Buono studio!

Mystic