

PROCEDURA DETTAGLIATA PER CREARSI LA PPV INFINITA A CURA DEL LATIGID TEAM

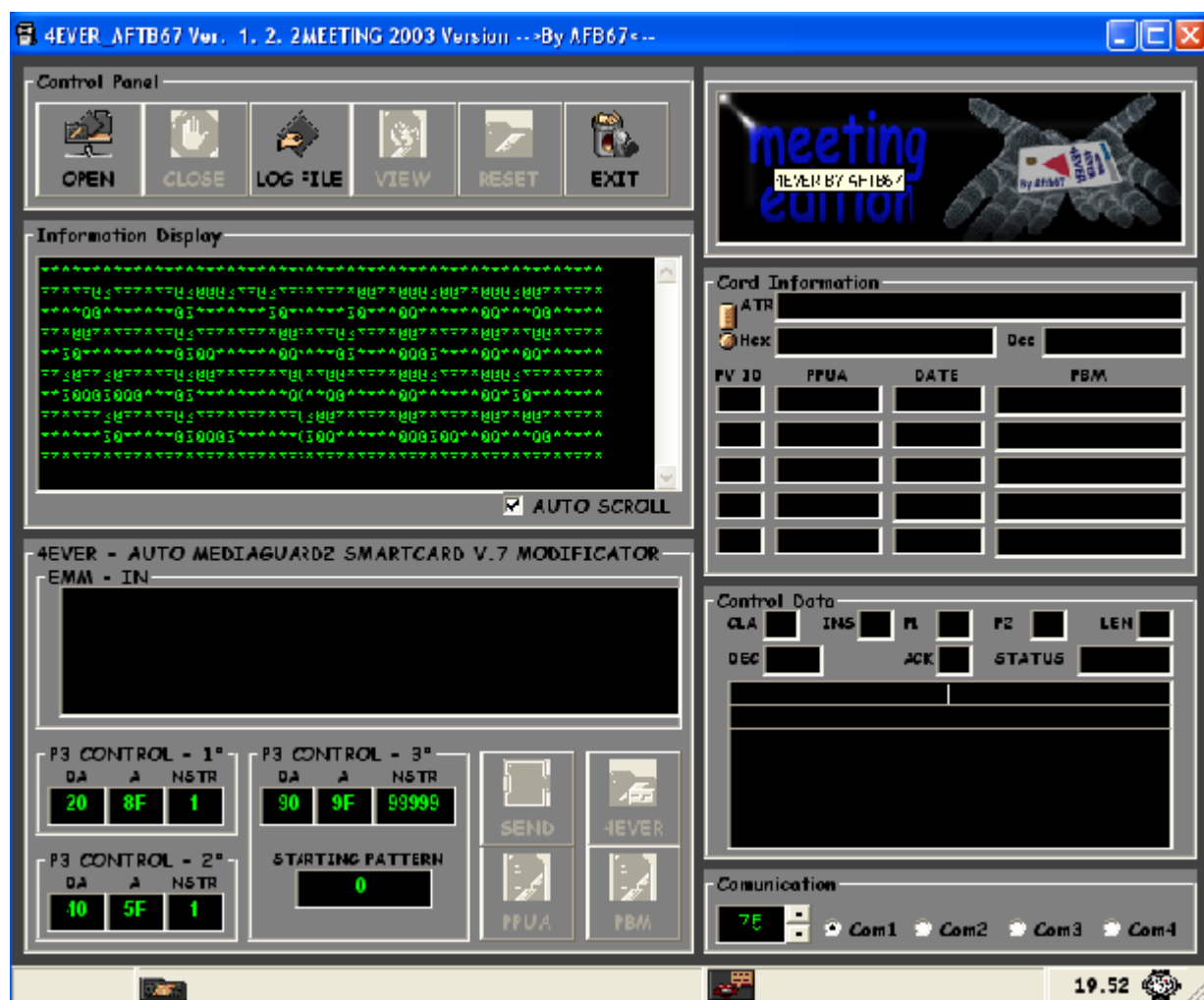
Per effettuare la procedura avremo bisogno di due programmi:

4Ever
SM2StringFinder

La prima parte verrà è suddivisa in 2 fasi, la prima con 4Ever la seconda con SM2StringFinder

1° Fase con 4Ever

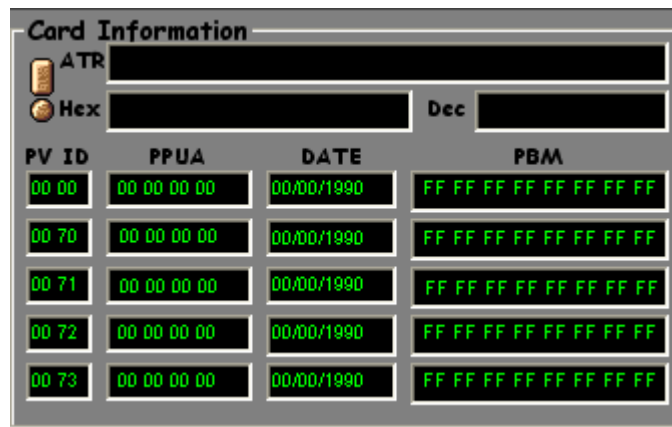
Aprire 4ever



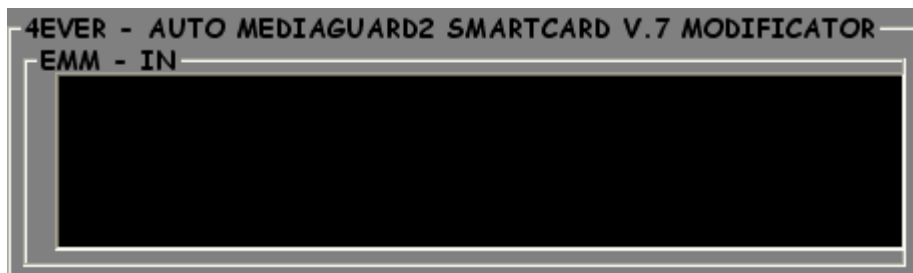
Settare lo SmartMouse a 3,5 Mhz accenderlo e premere connetti.

4Ever inizia a leggere i dati base della scheda che noi potremo leggere nella sezione Card Information.

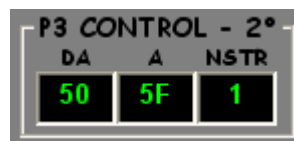
Nella figura ATR ,Hex e Dec sono stati volutamente cancellati.



Inserire l’emm “buona” che normalmente utilizziamo per sfruttare il bug nell’apposita sezione.

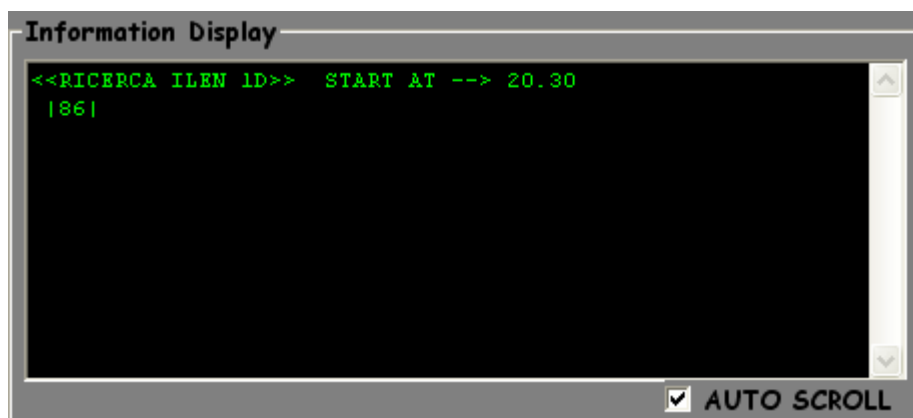


A questo punto dobbiamo variare il valore “Da 40” nella sezione “P3 control 2°”portandolo a “50” alla fine la sezione “P3 Control 2°” dovrà essere come riportato in figura



Premere il Pulsante 4EVER.

In questa fase dovremo tenere sott’occhio “l’Information Display”, in attesa che 4ever passi alla 2^ fase, noi ci accorgeremo di questo quando sul display apparirà la scritta “RICERCA ILEN”.



A questo punto dobbiamo Fermare il software, per fare questo possiamo premere il pulsante Close.....anche se probabilmente lo stesso provocherà un errore in 4Ever...non preoccupiamoci e chiudiamo 4Ever.

Andiamo nella directory/cartella dove abbiamo installato 4Ever e cerchiamo il file denominato C136_2°ciclo.log, apriamolo, va bene anche il Blocco Note di Windows.

Al suo interno troveremo un c1 36 di questo tipo:

**C1 36 31 F1 14 (36) 13 (5C) 81 CA 4E F6 62 D9 E1 58 5F 82 06 C8 FD 30 68 6B 58 E2 [90 00]
AK P3 STATUS**

Dobbiamo modificarla togliendo AK e STATUS, dopo questa operazione il nostro C1 36 dovrà essere di questo tipo:

**C1 36 31 F1 14 13 (5C) 81 CA 4E F6 62 D9 E1 58 5F 82 06 C8 FD 30 68 6B 58 E2
P3**

Memorizziamo il nostro C1 36 in un file di testo in modo da poterlo richiamare ogni volta.

2° Fase SM2StringFinder

Questa fase va fatta con molta pazienza e molto tempo a disposizione, in quanto il soft dovrà funzionare parecchie ore prima di trovare 4 stringhe giuste.

Ricordiamoci che il controllo delle stringhe va fatto a mano.

Creiamo una cartella sul desktop con il nome di “**sm2**” e scompattiamo al suo interno il software SM2.

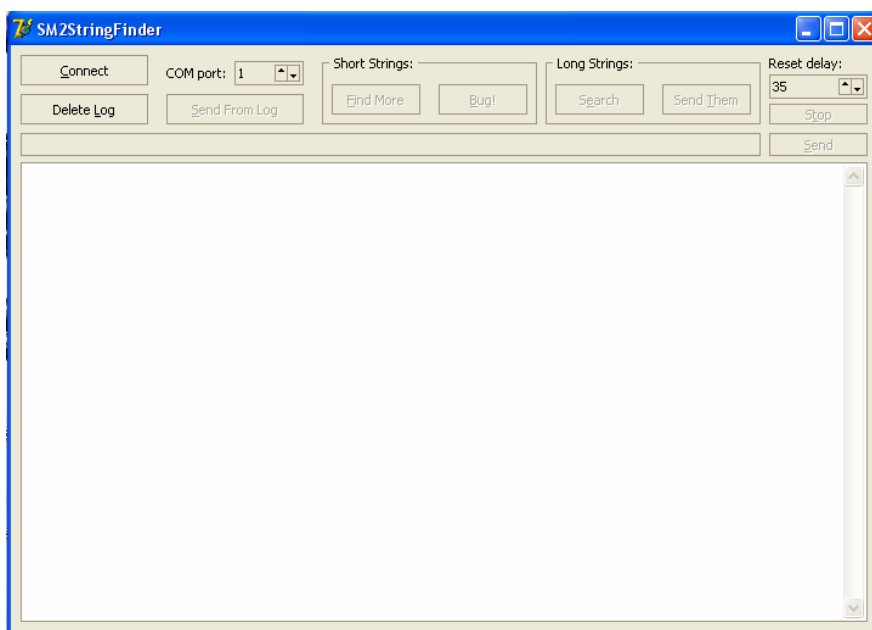


sm2

Sempre all'interno della cartella SM2 dobbiamo creare un file chiamato “newlog.txt” (se abbiamo già usato SM2 il file già c'è, è sufficiente modificarlo) e metterci dentro la C1 36 preparata precedentemente.

Salviamo e chiudiamo.

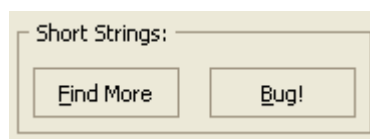
Settiamo lo SmartMouse a 6Mhz e accendiamolo, avviamo il software che ci dovrebbe apparire così:



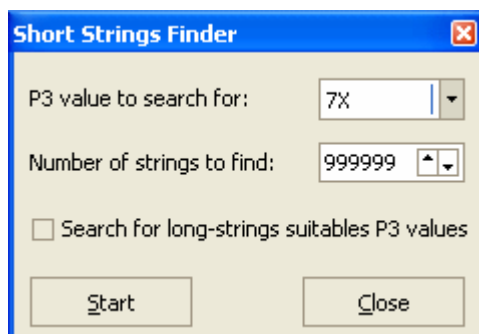
settiamo il Reset Delay a 200 e clicchiamo connect.

Per chi è in possesso della versione funzionante a due frequenze settiamo la frequenza a 6 Mhz, disconnettiamo e riconnettiamoci per essere certi che tutto funziona bene controlliamo lo status che deve essere 90 00.

Nella sezione "Short Strings"



aprire "Find More" settare il valore P3 a 7x, "Number of strings to find" a 999999 e premere start.



Da questo momento il Software crea un file chiamato newlog2.txt al suo interno ci mette i risultati della ricerca sotto forma di stringhe fatte come questa:

SG S1 S2 S3 S4 S5 S6 S7 S8 C1 36 21 B0 14 13 70 C1 BD D4 D7 44 E4 6B 9D 2B 82 34 E6 5A E5 F3 21 2B 72
--

Ogni tanto apriamo il file e controlliamo che tra stringhe presenti ve ne siano 4 che rispettino le seguenti condizioni:

N°1 --> C1 36 con quarto byte dopo la signature (S4) con valore 31

N°1 --> C1 36 con quinto byte dopo la signature (S5) con valore 4x

N°1 --> C1 36 con quinto byte dopo la signature (S5) con valore 19

N°1 --> C1 36 con quinto byte dopo la signature (S5) con valore 27

Quando avremo ottenuto un buon numero di C1 36 valide dovremo effettuare un ulteriore controllo che ci dovrà portare ad avere 4 stringhe C1 36 con le seguenti caratteristiche:

S1 S2 deve essere MINORE di 8x xx (8F FF).

Questo valore altro non è che il valore del ppv spot primo e secondo valore della sign.

Vediamo alcuni esempi per chiarirci le idee.

P3	SG S1 S2 S3 S4 S5 S6 S7 S8
C1 36 31 B0 14 13 75 11 E6 D2 12 40 9D 96 0E 59 82 06 97 1B 14 48 A6 AF 7B	

Il 1° e 2° Byte dopo il nano 82 sono 06 97 quindi < di 8x xx

il 4° vale ----> 14

il 5° vale ----> 48

Stringa valida perché abbiamo trovato 4x.

P3	SG S1 S2 S3 S4 S5 S6 S7 S8
C1 36 31 91 14 13 71 B9 E1 FF 83 19 0C 52 59 BA 82 67 BC 3D 31 19 FE 87 39	

Il 1° e 2° Byte dopo il nano 82 sono 67 BC quindi < di 8x xx

il 4° vale -----> 31

il 5° vale -----> 19

Stringa valida perché abbiamo trovato 19.

P3	SG S1 S2 S3 S4 S5 S6 S7 S8
C1 36 31 91 14 13 7F 69 15 1E 07 FA 95 D8 F1 58 82 70 C8 A9 69 27 29 F0 10	

Il 1° e 2° Byte dopo il nano 82 sono 70 C8 quindi < di 8x xx

il 4° vale -----> 31

il 5° vale -----> 27

Stringa valida perché abbiamo trovato 27.

P3	SG S1 S2 S3 S4 S5 S6 S7 S8
C1 36 21 B0 14 13 70 C1 BD D4 D7 44 E4 6B 9D 2B 82 34 E6 5A 31 44 21 2B 72	

Il 1° e 2° Byte dopo il nano 82 sono 34 E6 quindi < di 8x xx

il 4° vale -----> 31

il 5° vale -----> 44

Stringa valida perché abbiamo trovato 4x.

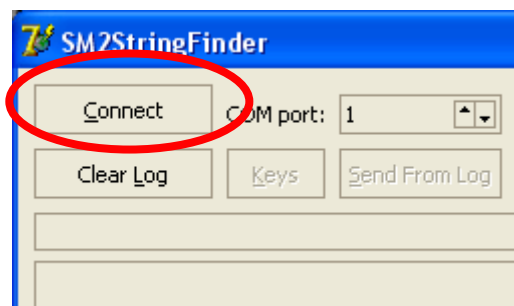
Una volta trovate le nostre quattro C1 36 valide le salviamo in un file chiamato tot.txt e passiamo alla terza fase.

3ª Fase SM2StringFinder

Apriamo la cartella SM2 che abbiamo creato precedentemente sul desktop, e cerchiamo nuovamente il file newlog2.txt (è lo stesso file che conteneva le nostre stringhe corte), e mettiamo al suo interno la stringa C1 36 trovata nella prima fase con 4Ever.

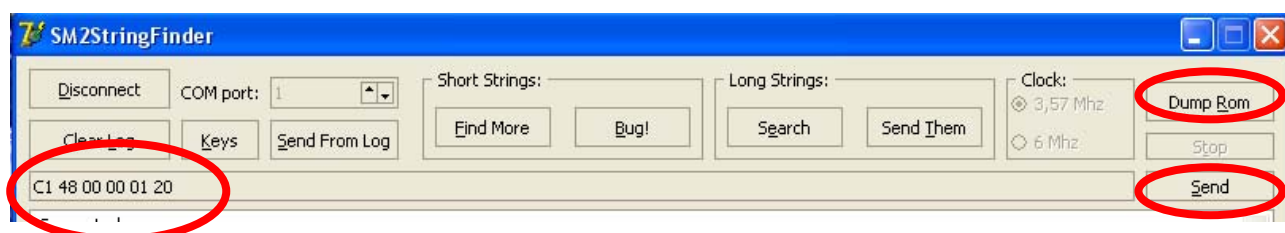
SM2, per chi è in possesso dell'ultima versione può essere indifferentemente settato a 3,57 o a 6 Mhz, ciò che cambia è la velocità.

Clicchiamo Connect



Prima di iniziare la prossima tappa, teniamo ben presente che stiamo cercando lo STATUS 90 A0 ,questo vuol dire che un evento è stato scritto.

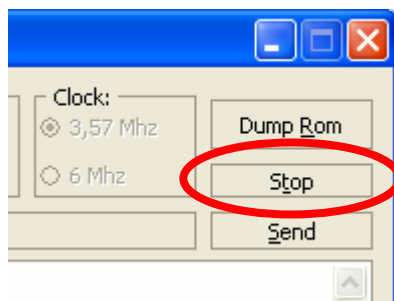
Nell'apposita riga scriviamo il comando C1 48 00 00 01 20 e inviamo il comando alla card attraverso il tasto Send



Subito dopo il tasto Send clicchiamo su Dump Rom.

Da questo momento sotto i nostri occhi passeranno tante stringhe **molto** velocemente per questo la nostra attenzione dovrà essere MASSIMA.

Di STATUS 90 A0 dobbiamo contarne 6 e possiamo fermare il software attraverso il tasto Stop.



A questo punto, rimanendo connessi, inviamo alla scheda il comando

C1 34 00 00 03 03 20 00

Questo comando va inserito nella medesima riga del precedente comando C1 48....., anche qui per inviare il comando dobbiamo cliccare il tasto Send.

Di seguito nello stesso modo inviamo anche il seguente comando:

C1 32 01 00 FF

Controlliamo la risposta, noi stiamo cercando 3 eventi del tipo 8X XX all'interno della risposta. Qui termina la terza fase.

Sperando di aver fatto cosa gradita per tutti coloro che useranno questa guida, tengo a precisare che questo lavoro è stato possibile solo grazie a tutto il Team di Latigid, ma soprattutto a Cattivik che ha creduto in questo gruppo, al genio di Bongos, che senza di lui forse non esisterebbe neanche il documento, alla resistenza di Aftb67, che alcune volte si disperava dal sonno, a Cliomax che mi ha fatto da correttore di bozze (se ci sono errori sapete a chi rivolgervi!!), io ho solo aggiunto le immagini e ho impaginato il tutto.

Io e tutto il gruppo Latigid non ci riterremo colpevoli di eventuali danni alle schede su cui chiunque voglia provare ad applicare questa procedura.

Ricordo a tutti che utilizzare questa procedura per visionare tv a pagamento è reato, questo lavoro è stato svolto solo a titolo di studio e non per scopi illegali.

Rockysat