Come modificare la TOC

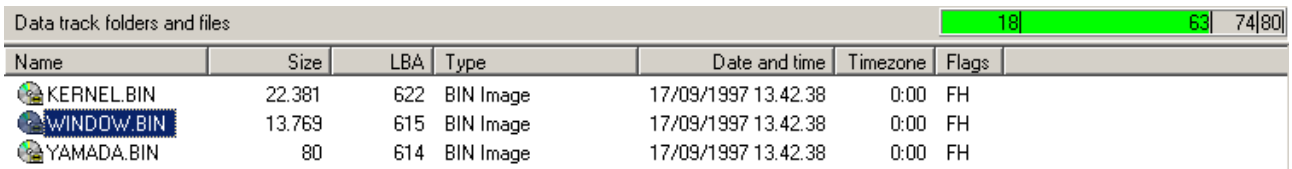
Il fine di questa guida è spiegare come modificare la TOC (Table of Contenents), per poter inserire in un iso un file leggermente superiore alla sua grandezza originaria (purché si tratti di pochi kb, ma dovreste sapere che con pochi kb si fanno miracoli, soprattutto con files compressi).
Questa guida è comunque ormai "pragmaticamente" inutile, data la pubblicazione del TOC Changer di Phoenix (che trovate sul nostro sito)... la sto rimettendo online per i più curiosi di voi. ;)

NOTA: Quando scrissi questa guida, non sapevo che Final Fantasy VII avesse una "seconda TOC" nascosta nel file YAMADA.BIN.
Per poter espandere correttamente il WINDOW.BIN ED IL KERNEL.BIN occorre modificare questo file, contenente l'LBA e le dimensioni dei file più importanti del gioco.
Inoltre, si fa presente che l'espansione della TOC potrebbe NON funzionare, qualora si lavorasse con giochi che adoperano indici, pur mantenendo una TOC standard (esempio: Legend of Mana).

Perdonate questi "peccati di gioventù". :P

1. Cos'è la TOC, ed a cosa serve?

Come il nome dice, la TOC non serve ad altro che ad "indicare" dove sono i files all'interno di un cd ed ad indicarne le varie proprietà (grandezza, dimensione e così via…).
Il nostro scopo è quello di modificarla, per poter reinserire un file leggermente più grande dell'originale.
Prendiamo come esempio il file **WINDOW.BIN** di **Final Fantasy 7** (contenuto nella cartella \INIT\), contenente la maggior parte della grafica del menu del gioco.


Data track folders and files

18 63 74 80

Name	Size	LBA	Type	Date and time	Timezone	Flags
KERNEL.BIN	22.381	622	BIN Image	17/09/1997 13.42.38	0:00	FH
WINDOW.BIN	13.769	615	BIN Image	17/09/1997 13.42.38	0:00	FH
YAMADA.BIN	80	614	BIN Image	17/09/1997 13.42.38	0:00	FH

Come potete vedere, la TOC indica che grandezza attuale del file è 13'769 bytes.
Supponiamo di ritrovarci, dopo averlo editato e ricompresso, un file più grande, per l'esattezza di 13'900 bytes.
Come fare a reinserirlo?
Semplice, basterà modificare la TOC, facendo in modo che indichi che la grandezza del **WINDOW.BIN** non sia più di 13769, bensì 13900 bytes.

2. Come modificare la TOC

Eccoci qui, nella parte più importante di questa piccola e, spero utile, guida.
Innanzitutto vi serviranno i seguenti programmi:

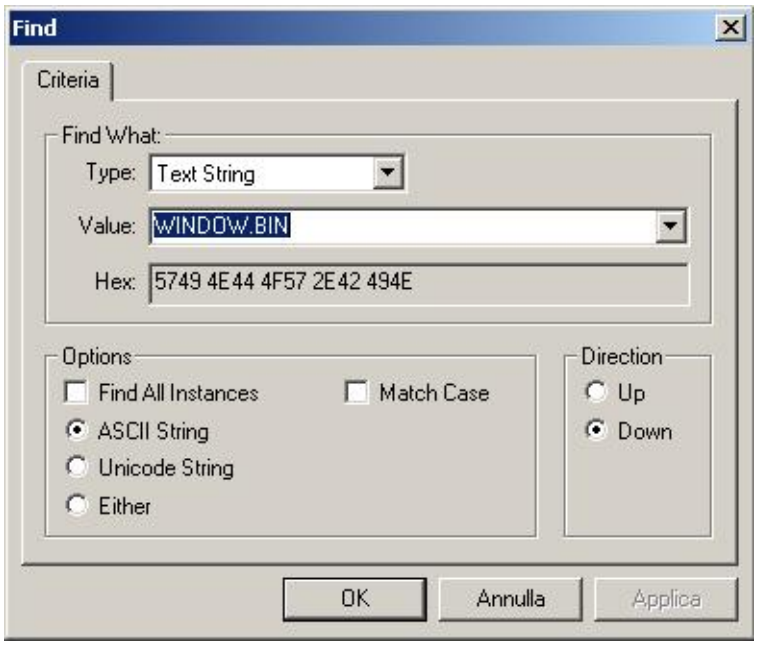
- **Hex Workshop** (una qualsiasi versione va bene)
- **Transhlextion 1.6c**
- **CDMage versione 1.02.1** (non serve a modificare la **TOC**, ma è ottimo per reinserire files in un iso)

Una volta accertato di possederli tutti, è ora di divertirsi!

Nota: le operazioni sotto descritte possono, ovviamente, essere realizzate anche con diversi programmi, magari che permettono di modificare direttamente un file iso, come **WinHex** od il **ThingyV2**.
Le operazioni da compiere sono, ovviamente, le stesse.
Io mi trovo bene col metodo che sto per illustrarvi, però poi è scelta vostra… dopotutto l'importante è la modifica alla TOC!

Passo numero 1: Trovare nell'iso le informazioni relative al file

Questa è un'operazione assai semplice.
Segnatevi il nome del file da cercare (nel nostro caso **WINDOW.BIN**), ed a questo punto aprite con **HexWorkshop** il file immagine, ed immettete come parametro di ricerca (testo) il nome del file.

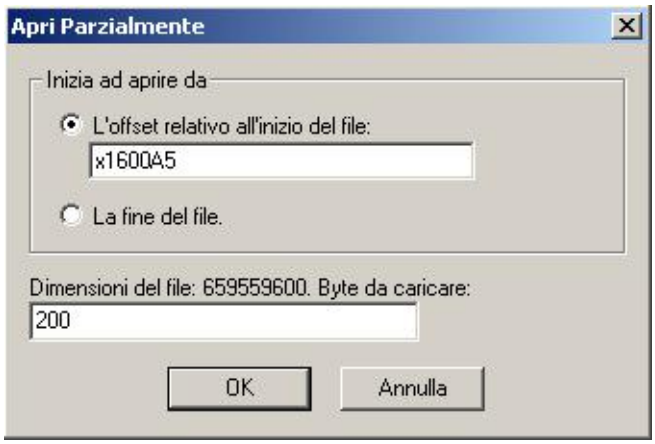


Una volta trovato il nome del file, segnatevi il suo offset (nel nostro caso 0x1600C5), sottraendo però al totale circa $20 (con xNumero o $numero intendo bytes hex), poi capirete perché.

Passo numero 2: Modificare la TOC

Eccoci arrivati al cuore dell'operazione…ora prestate molta attenzione.
Innanzitutto segnatevi quanto è grande il file originale (nel nostro caso 13'769 bytes), ed a questo punto **convertite la cifra decimale in esadecimale** (usate la calcolatrice di Windows in modalità Avanzata)**.**
13769 diviene, ad esempio, 35C9.
Compiuta questa operazione, **invertite la cifra esadecimale ottenuta** (ricordatevi che un byte hex è formato da due simboli numerici, ad esempio 6D è un byte).
35C9 diviene perciò C935.
La stessa operazione è da farsi con il file modificato, accertandovi di segnare la grandezza in hex di ambedue i numeri, invertita e non.

Adesso, col **Transhlextion**, utilizzate il comando "Apri parzialmente", e dite al programma di caricare un 200 bytes, partendo dall'offset che avevate trovato con **HexWorkshop**, ricordandovi di sottrarre x20.



Fatto ciò, cercate nei bytes precedenti al nome del file **la grandezza in hex del file originale, sia coi bytes invertiti che con quelli "originali".**

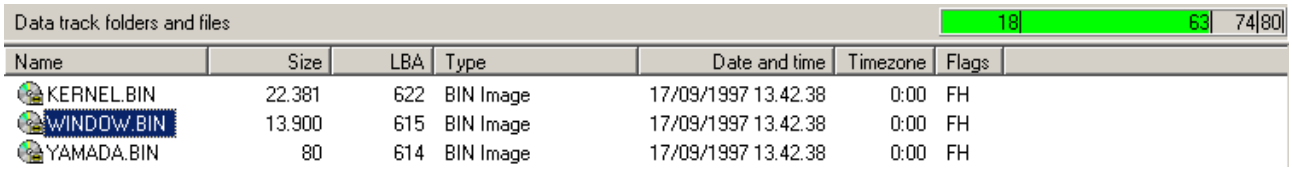
Noterete subito che nei 20 bytes precedenti al nome (capite ora perché prima vi ho fatto fare la sottrazione di $20 dall'offset?) vi saranno entrambe le coppie:

La coppia invertita…

```
00000000  00 67 02 00 00 00 00 02 67 C9 35 00 00 00 00 35  .g......gÉ5....5
00000010  C9 61 09 11 15 2A 26 24 01 00 00 01 00 00 01 0C  Éa...*&$........
00000020  57 49 4E 44 4F 57 2E 42 49 4E 3B 31 00 2A 00 2A  WINDOW.BIN;1.*.*
00000030  00 08 01 58 41 00 00 00 00 00 00 3C 00 66 02 00  ...XA......<.f..
00000040  00 00 00 02 66 50 00 00 00 00 00 00 50 61 09 11  ....fP......Pa..
00000050  15 2A 26 24 01 00 00 01 00 00 01 0C 59 41 4D 41  .*&$........YAMA
00000060  44 41 2E 42 49 4E 3B 31 00 2A 00 2A 00 08 01 58  DA.BIN;1.*.*...X
00000070  41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  A...............
00000080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000C0  00 00 00 00 00 00 00 00                          ........
```

e quella NON invertita:

Trovate le coppie, siete oramai in prossimità del traguardo.
Modificate le cifre esadecimali (**sia** quella invertita che quella "normale"), sostituendo alle originali quelle del file più grande (esempio: al posto di **35C9** mettete **364C**), e, compiuta l'operazione, andate a controllare nel CD la grandezza attuale del file…



Il file si è "magicamente" espanso, passando da 13769 bytes a 13900.
In realtà il file è rimasto identico, è stata la TOC ad essere stata modificata, indicando che il file è grande 13900 bytes, mentre i bytes effettivi sono 13769.
Comunque, anche lasciando il file originale intatto con la TOC modificata non si otterrebbe nessun problema, poiché i bytes in più non sono altro che degli 00.

In realtà, in un cd, tra un file ed un altro ci sono (quasi) moltissimi byte 00 inutilizzati, che possono essere sfruttati liberamente, una volta modificata la TOC (cosa che spero siate riusciti a fare senza problemi!).
Adesso non vi resta che reinserire comodamente il file con **CdMage** e testare il vostro file espanso…

Questo è tutto, gente! :D

3. Note

Già che ci sono vi do qualche piccola dritta…

Innanzitutto, vi consiglio di modificare la TOC in modo che possa contenere anche un file più grande di quello modificato…sapete, magari vi ritroverete a modificarlo di nuovo, ingrandendolo ancora, ed allora vi ringrazierete per aver "espanso" più del dovuto.

Seconda cosa…troverete questa operazione utile **soprattutto** modificando dati compressi, dove capita spesso di trovarsi con files ricompressi leggermente più grandi del normale…
Sarà allora che la modifica alla TOC sarà vitale; vi permetterà di fare cose prima impensabili…
Pensate quanto è frustante ritrovarsi con un file di pochissimi bytes più grande, impossibile da reinserire!
E qui la modifica alla TOC dà il meglio di sé.

Ultimo consiglio …la TOC, ovviamente, non potrà "espandere" all'infinito un file, poiché, ingrandendo troppo, si rischia di sovrascrivere il file successivo oppure gli **ECD/ECC** che riguardano il file che dobbiamo espandere.
Per controllare la dimensione massima raggiungibile basta un piccolo calcolo, nient'altro che una sottrazione di due **LBA** (conosciuti anche come **Block**) e di una moltiplicazione per 2048 (che nello standard **ISO9600** sono i bytes per settore).
Non sono da contarsi infatti gli ultimi 304 bytes per settore in un file immagine **RAW**.
La formula è questa:

LBA 1 = file da espandere
LBA 2 = file successivo a quello da espandere

(LBA 2 – LBA 1) · 2048 = risultato massimo

Prendendo come esempio il WINDOW.BIN ed il successivo KERNEL.BIN...

(622 – 615) · 2048 = 7 · 2048 = 14336.

Dunque il WINDOW.BIN non potrà avere dimensione maggiore di 14336 bytes.

4. Congedo

Beh, eccovi giunti alla conclusione di questa breve e, spero, esauriente guida.
Credo di essere riuscito a scriverla senza fare apparire l'operazione troppo difficile (in realtà è facilissima) e, soprattutto, spero che questa piccola ma utilissima operazione possa aiutarvi nell'hacking di giochi su CD che utilizzano una normale TOC.

Un grandissimo ringraziamento a **Gemini**, il quale mi spiegò come modificarla, permettendomi di modificare agevolissimamente alcuni files compressi di **Final Fantasy 7** contenenti varia grafica.

Altro grande ringraziamento ad **Auryn**, che mi ha suggerito di inserire nella guida il piccolo calcolo per scoprire immediatamente la grandezza massima che può avere il file da espandere.
Devo ammettere che sono stato alquanto distratto a non pensarci prima!

Sephiroth 1311

5. Disclaimer