ИСКАЖЕНИЕ TOC КАК СРЕДСТВО БОРЬБЫ С НЕСАНКЦИОНИРОВАННЫМ КОПИРОВАНИЕМ ДИСКА

Уже давно
Утихло поле боя,
Но сорок тысяч
Воинов Китая
Погибли здесь,
Пожертвовав собою...
Ду Фо
«Оплакиваю поражение при Чэньтао»

Искажение TOC – жестокий, уродливый но на удивление широко распространенный прием, использующийся в доброй половине защитных механизмов. Штатные копировщики на таких дисках в буквальном смысле слова сходят с ума и едут крышей. Копировщики защищенных дисков (Clone CD, Alcohol 120%) к искаженному TOC относятся гораздо лояльнее, но требуют для своей работы определенного сочетания пишущего и читающего приводов, да и в этом случае копируют такой диск не всегда.

КРИС КАСПЕРСКИ

Пишущий привод обязательно должен поддерживать режим RAW DAO (Disc At Once), в котором весь диск записывается за один проход лазера. Режим RAW SAO (Session At Once) для этих целей совершенно непригоден, поскольку предписывает приводу писать сначала содержимое сессии, а потом – TOC. Как следствие – приводу приходится самостоятельно анализировать TOC, чтобы определить стартовый адрес сессии и ее длину. Попытка записать искаженный TOC в режиме SAO в общем случае приводит к непредсказуемому поведению привода и о работоспособной копии защищенного диска нечего и думать! Первая встретившаяся приводу сессия с искаженным TOC обычно оказывается и последней, т.к. остальные сессии писать уже некуда (искажение TOC обычно преследует цель увеличения размера сессии до нескольких гигабайт).

Читающий привод помимо режима «сырого» чтения (который поддерживают практически все приводы) должен уметь распознавать искаженный TOC, автоматически переходя в этом случае на использование «резервного» средства адресации – Q-канала подкода. В противном случае сессия, содержащая искаженный TOC, окажется недоступной для чтения даже на секторном уровне.

Таким образом, копирование дисков с искаженным TOC осуществимо не на всяком оборудовании и порядка 1/3 моделей «писцов» для этих целей непригодны. Узнать, поддерживает ли выбранная вами модель привода режим RAW DAO или нет, можно, в частности, из раздела «Tech support» справки Clone CD, где перечислены характеристики достаточно большого количества всевозможных приводов (впрочем, моих приводов там, увы, нет). Другой путь – «скормить» приводу SCSI/ATAPI команду 46h (GET CONFIGURATION) и посмотреть, что он ответит. Из двух моих «писцов» режим RAW DAO поддерживает один лишь NEC. С определением возможности чтения искаженных сессий дела обстоят на порядок сложнее, ибо данная особенность поведения является исключительно внутренней характеристикой привода и не афишируется ни самим приводом, ни его производителями. Приходится выяснять эту информацию экспериментально. Возьмите диск с чудовищно искаженным TOC (о том, как его создать, рассказано ниже), воткните его в привод и попробуйте прочесть несколько секторов из искаженной сессии. Реакция приводов может быть самой разнообразной. Тот же PHILIPS в зависимости от «настроения» своих электронных цепей то рапортует об ошибке чтения, то возвращает совершенно бессмысленный мусор, в котором не угадывается даже синхропоследовательность, возглавляющая заголовок сырого сектора.

Основной недостаток защитных механизмов с искаженным TOC состоит в том, что некоторые приводы такие диски просто «не видят» и потому не могут их воспроизвести. Легальный пользователь, испытавший несовместимость защиты со своей аппаратурой, в лучшем случае обложит ее разработчика матом и поспешит вернуть диск продавцу… если, конечно, сможет вытащить эту «бяку» из недр CD-ROM, и не факт, что у него получится, поскольку микропроцессорная начинка некоторых приводов при попытке анализа искаженного TOC просто «зависает» и привод полностью абстрагируется от всех раздражителей внешнего мира, не реагируя в том числе и на настойчивые попытки пользователя сделать диску «EJECT». Дырку для аварийного выброса диска, правда, еще никто не отменял[1], но, по слухам, не везде она есть (хотя лично мне приводов без дырки еще не встречалось), а там где есть – зачастую оказывается скрытой за декоративной панелью или – что более вероятно – пользователь может вообще не знать, что это за отверстие такое, для чего оно предназначено и как им, собственно, следует пользоваться. На «Макинтошах» таких дырок нет – это точно (или же «Маковские» пользователи все сплошь идиоты). Во всяком случае, количество судебных исков, поданных последними, в буквальном смысле слова не поддается ни разуму, ни исчислению. Самое интересное, что подавляющее большинство этих исков были удовлетворены и разработчикам пришлось оплатить и «ремонт» аппаратуры, и моральный ущерб, и собственно сами судебные издержки. (Между нами говоря, снятие защиты с дисков, записанных с грубыми нарушениями стандарта, коими, в частности, и являются диски с искаженным TOC, не считается взломом, и не преследуется по закону, поэтому ломайте, ломайте и еще раз ломайте).

Создание защищенного диска с искаженным TOC

Для создания защищенного диска с искаженным TOC нам понадобится: любая программа записи на диск, умеющая создавать многосессионные диски (например, Roxio Easy CD Creator), копировщик защищенных дисков, сохраняющий содержимое TOC в текстовом файле, доступном для редактирования (мы выбираем Clone CD), и, естественно, сам пишущий привод, поддерживающий режим сырой записи в режиме DAO. Для облегчения восприятия материала все действия будут расписаны по шагам, хотя это выглядит и не слишком литературно.

Шаг первый

Достаем из упаковки CD-R болванку или – что даже лучше – засовываем в привод потертый жизнью CD-RW диск и записываем на него пару сессий в штатном режиме. Будет лучше (вернее, нагляднее), если вторая сессия будет включать в себя файлы первой сессии – той самой сессии, чей TOC мы и собираемся искажать. Интересно, сможет ли привод прочесть ее содержимое или нет?

Шаг второй

Запускаем Clone CD и просим его создать образ оригинального диска (выбираемый профиль настроек на данном этапе некритичен, поскольку диск еще не защищен, то с равным успехом можно использовать как «CD с данными», так и «Protected PC Game»; галочку «создавать Cue-Sheet» взводить необязательно – все равно она действительна лишь на односессионных CD).

Шаг третий

Если все сделано правильно и программно-аппаратное обеспечение во всей своей совокупности работает нормально, на жестком диске должны образоваться три файла: IMAGE.CCD, – несущий в себе содержимое Q-канала подкода Lead-In области или, попросту говоря, TOC;

IMAGE.IMG – «сырой» образ диска со всеми секторами от 00:00:02 до «сколько-на-диске-есть-там» и IMAGE.SUB – содержимое полей подкода «программной» части диска. Последний файл в принципе может и отсутствовать (он создается только, если взведена галочка «Чтение субканалов из треков с данными»), но это некритично, т.к. сейчас нас в первую очередь интересуют не каналы подкода, а сам TOC!

Откроем файл IMAGE.CCD в любом текстовом редакторе и попытаемся перевести расклад геометрии диска на человеческий язык.

Листинг 1. Содержимое неискаженного TOC в сыром виде. Обобщенно говоря, диск содержит две секции – по одному треку каждая. Абсолютный адрес начала первого трека 00:00:02, абсолютный адрес Lead-out-области первой сессии 00:29:33 (адрес последнего сектора трека на две секунды короче), абсолютный адрес начала второго трека 03:01:33, а абсолютный адрес Lead-out второй сессии 03:24:33. Максимально достижимая емкость диска 22:14:34 (хотя на самом диске и написано, что он 23-минутный).

```
[CloneCD]                ; данные о Clone CD
Version=3                ; версия Clone CD.

[Disc]                   ; данные диска
TocEntries=12            ; количество элементов TOC
Sessions=2               ; количество сессий = 2
DataTracksScrambled=0    ; поле DVD (см. inf-8090), для CD
                         ; эта информация лишена смысла
CDTextLength=0           ; CD-Text в полях подкода
                         ; Lead-in-области отсутствует
[Session 1]       ; данные сессии 1
PreGapMode=1      ; тип трека Mode 1 (трек с данными,
                  ; 2048 байт данных)
PreGapSubC=0      ; данных подканала нет

[Session 2]       ; данные сессии 2
PreGapMode=1      ; тип трека Mode 1 (трек с данными,
                  ; 2048 байт данных)
PreGapSubC=0      ; данных подканала нет

[Entry 0]         ; данные элемента TOC №0
Session=1         ; элемент сессии 1
Point=0xa0        ; номер первого трека сессии 1
                  ; в PMin/тип диска в PSec
ADR=0x01          ; q-Mode == 1
Control=0x04      ; диск с данными, запрещенный
                  ; для копирования
TrackNo=0         ; трек, который мы сейчас читаем, -
                  ; это Lead-in-трек (т.е. TOC)
AMin=0            ; \
ASec=0            ;  + абсолютный адрес текущего трека
AFrame=0          ; /
ALBA=-150         ; LBA-адрес текущего трека
Zero=0            ; это поле должно быть равно нулю,
                  ; как оно и есть
PMin=1            ; номер первого трека сессии 1
PSec=0            ; тип диска CD-DA и CD-ROM-диск в Mode 1
PFrame=0          ; не несет никакой полезной информации
PLBA=4350         ; номер трека, представленный Clone CD
                  ; как LBA-адрес, т.е. глупость
[Entry 1]         ; данные элемента TOC №1
Session=1         ; элемент сессии 1
Point=0xa1        ; номер последнего трека сессии 1 в PMin
ADR=0x01          ; q-Mode == 1
Control=0x04      ; диск с данными, запрещенный
                  ; для копирования
TrackNo=0         ; трек, который мы сейчас читаем, -
                  ; это Lead-in-трек (т.е. TOC)
AMin=0            ; \
ASec=0            ;  + абсолютный адрес текущего трека
AFrame=0          ; /
ALBA=-150         ; LBA-адрес текущего трека
Zero=0            ; это поле должно быть равно нулю,
                  ; как оно и есть
PMin=1            ; номер последнего трека сессии 1
                  ;(в сессии только один трек)
PSec=0            ; не несет никакой полезной информации
PFrame=0          ; не несет никакой полезной информации
PLBA=4350         ; номер трека, представленный Clone CD
                  ; как LBA-адрес, т.е. глупость
[Entry 2]         ; данные элемента TOC №2
Session=1         ; элемент сессии 1
Point=0xa2        ; положение Lead-out-области
                  ; в PMin:PSec:PFrame
ADR=0x01          ; q-Mode == 1
Control=0x04      ; диск с данными, запрещенный
                  ; для копирования
TrackNo=0         ; трек, который мы сейчас читаем, -
                  ; это Lead-in-трек (т.е. TOC)
AMin=0            ; \
ASec=0            ;  + - абсолютный адрес текущего трека
AFrame=0          ; /
ALBA=-150         ; LBA-адрес текущего трека
Zero=0            ; это поле должно быть равно нулю,
                  ; как оно и есть
PMin=0            ; \
PSec=29           ;  + - абсолютный адрес Lead-out-области
                  ;      сессии 1
PFrame=33         ; /
PLBA=2058         ; LBA-адрес Lead-out-области сессии 1

[Entry 3]         ; данные элемента TOC №3
Session=1         ; элемент сессии 1
Point=0x01        ; данные трека 1 сессии 1
ADR=0x01          ; q-Mode == 1
Control=0x04      ; диск с данными, запрещенный
                  ; для копирования
TrackNo=0         ; трек, который мы сейчас читаем, -
                  ; это Lead-in-трек (т.е. TOC)
AMin=0            ; \
ASec=0            ;  + - абсолютный адрес текущего трека
AFrame=0          ; /
ALBA=-150         ; LBA-адрес текущего трека
Zero=0            ; это поле должно быть равно нулю,
                  ; как оно и есть
PMin=0            ; \
PSec=2            ;  + - абсолютный адрес начала трека 1
                  ;      сессии 1
PFrame=0          ; /
PLBA=0            ; LBA-адрес начала трека 1 сессии 1

[Entry 4]         ; данные элемента TOC №4
Session=1         ; элемент сессии 1
Point=0xb0        ; позиция следующий записываемой области
                  ; в AMin:ASec:AFrame
ADR=0x05          ; q-Mode == 1
Control=0x04      ; диск с данными, запрещенный
                  ; для копирования
TrackNo=0         ; трек, который мы сейчас читаем, -
                  ; это Lead-in-трек (т.е. TOC)
AMin=2            ; \
ASec=59           ;  + - абсолютный адрес следующей
                  ;      записываемой области
AFrame=33         ; /
ALBA=13308        ; LBA-адрес следующей записываемой области
Zero=3            ; кол-во pointer в Mode 5
PMin=22           ; \
PSec=14           ;  + - абсолютный адрес максимальной
                  ;      записываемой области
PFrame=34         ; /
PLBA=99934        ; LBA-адрес максимальной записываемой
                  ; области
[Entry 5]         ; данные элемента TOC №5
Session=1         ; элемент сессии 1
Point=0xc0        ; стартовый адрес Lead-in-области
                  ; Hybrid-диска (если он есть)
ADR=0x05          ; Mode 5 (Оранжевая книга)
Control=0x04      ; диск с данными, запрещенный
                  ; для копирования
TrackNo=0         ; трек, который мы сейчас читаем, -
                  ; это Lead-in-трек (т.е. TOC)
AMin=162          ; рекомендуемая мощность лазера для записи
ASec=128          ; Application code
AFrame=140        ; зарезервировано
ALBA=288590       ; LBA-"адрес" трех предыдущих полей
Zero=0            ; зарезервировано
PMin=97           ; \
PSec=27           ;  + - абсолютный адрес Lead-in-области
                  ;      Hybrid-диска
PFrame=21         ; /    (адрес лежит за пределами диска,
                  ;      т.е. Hybrid-диска нет)
PLBA=-11604       ; LBA-адрес Lead-in-области Hybrid
                  ; (вычислен с переполнением)
[Entry 6]         ; данные элемента TOC №6
Session=1         ; элемент сессии 1
Point=0xc1        ; копия ATIP-информации
ADR=0x05          ; -+
Control=0x04      ; -+
```

```
TrackNo=0          ; -+
AMin=4             ; -+
ASec=120           ; -+
AFrame=96          ; -+
ALBA=26946         ; -+ - ATIP-информация
Zero=0             ; -+
PMin=0             ; -+
PSec=0             ; -+
PFrame=0           ; -+
PLBA=-150          ; -+

[Entry 7]          ; данные элемента TOC №7
Session=2          ; элемент сессии 2 (вот мы и добрались
                   ; до сессии 2!)
Point=0xa0         ; номер первого трека сессии 2
                   ; в PMin/тип диска в PSec
ADR=0x01           ; q-Mode == 1
Control=0x04       ; диск с данными, запрещенный
                   ; для копирования
TrackNo=0          ; трек, который мы сейчас читаем, -
                   ; это Lead-in-трек (т.е. TOC)
AMin=0             ; \
ASec=0             ;  + - абсолютный адрес текущего трека
AFrame=0           ; /
ALBA=-150          ; LBA-адрес текущего трека
Zero=0             ; это поле должно быть равно нулю,
                   ; как оно и есть
PMin=2             ; номер первого трека сессии 2
                   ; (нумерация треков сквозная!)
PSec=0             ; тип диска CD-DA и CD-ROM-диск в Mode 1
PFrame=0           ; не несет никакой полезной информации
PLBA=8850          ; номер трека, представленный Clone CD
                   ; как LBA-адрес, т.е. глупость
[Entry 8]          ; данные элемента TOC №8
Session=2          ; элемент сессии 2
Point=0xa1         ; номер последнего трека сессии 2 в PMin
ADR=0x01           ; q-Mode == 1
Control=0x04       ; диск с данными, запрещенный
                   ; для копирования
TrackNo=0          ; трек, который мы сейчас читаем, -
                   ; это Lead-in-трек (т.е. TOC)
AMin=0             ; \
ASec=0             ;  + - абсолютный адрес текущего трека
AFrame=0           ; /
ALBA=-150          ; LBA-адрес текущего трека
Zero=0             ; это поле должно быть равно нулю,
                   ; как оно и есть
PMin=2             ; номер последнего трека сессии 2
                   ; (в сессии только один трек)
PSec=0             ; не несет никакой полезной информации
PFrame=0           ; не несет никакой полезной информации
PLBA=8850          ; номер трека, представленный Clone CD
                   ; как LBA-адрес, т.е. глупость
[Entry 9]          ; данные элемента TOC №9
Session=2          ; элемент сессии 2
Point=0xa2         ; положение Lead-out-области
                   ; в PMin:PSec:PFrame
ADR=0x01           ; q-Mode == 1
Control=0x04       ; диск с данными, запрещенный
                   ; для копирования
TrackNo=0          ; трек, который мы сейчас читаем, -
                   ; это Lead-in-трек (т.е. TOC)
AMin=0             ; \
ASec=0             ;  + - абсолютный адрес текущего трека
AFrame=0           ; /
ALBA=-150          ; LBA-адрес текущего трека
Zero=0             ; это поле должно быть равно нулю,
                   ; как оно и есть
PMin=3             ; \
PSec=24            ;  + - абсолютный адрес Lead-out-области
                   ;      сессии 2
PFrame=23          ; /
PLBA=15173         ; LBA-адрес Lead-out-области сессии 2

[Entry 10]         ; данные элемента TOC №10
Session=2          ; элемент сессии 2
Point=0x02         ; данные трека 2 сессии 2
ADR=0x01           ; q-Mode == 1
Control=0x04       ; диск с данными, запрещенный
                   ; для копирования
TrackNo=0          ; трек, который мы сейчас читаем, -
                   ; это Lead-in-трек (т.е. TOC)
AMin=0             ; \
ASec=0             ;  + - абсолютный адрес текущего трека
AFrame=0           ; /
ALBA=-150          ; LBA-адрес текущего трека
Zero=0             ; это поле должно быть равно нулю,
                   ; как оно и есть
PMin=3             ; \
PSec=1             ;  + - абсолютный адрес начала трека 2
                   ;      сессии 2
PFrame=33          ; /
PLBA=13458         ; LBA-адрес начала трека 2 сессии 2

[Entry 11]         ; данные элемента TOC №11
Session=2          ; элемент сессии 2
Point=0xb0         ; адрес следующей записываемой области
                   ; в AMin:ASec:AFrame
ADR=0x05           ; Mode 5
Control=0x04       ; диск с данными, запрещенный
                   ; для копирования
TrackNo=0          ; трек, который мы сейчас читаем, -
                   ; это Lead-in-трек (т.е. TOC)
AMin=4             ; \
ASec=54            ;  + - абсолютный адрес следующей
                   ;      записываемой области
AFrame=23          ; /
ALBA=21923         ; LBA-адрес следующей записываемой области
Zero=1             ; количество pointer Mode 5
PMin=22            ; \
PSec=14            ;  + - абсолютный адрес последней
                   ;      возможной Lead-out-области
PFrame=34          ; /    (на самом диске написано 23 мин.,
                   ;      это ж как надо округлять 22:14:34)
PLBA=99934         ; LBA-адрес последней возможной
                   ; Lead-out-области
[TRACK 1]          ; данные трека 1
MODE=1             ; режим Mode 1
INDEX 1=0          ; post-gap?

[TRACK 2]          ; данные трека 2
MODE=1             ; режим Mode 1
INDEX 1=0          ; post-gap?
```

Давайте теперь немного поиздеваемся над TOC и увеличим стартовый адрес первого трека так, чтобы он вышел далеко за пределы первой сессии и попал… ну, собственно, куда нибудь он все равно попадет. Чтобы быстро отыскать соответствующую ему запись, воспользуемся контекстным поиском. Жмем <F7> и вводим «point=0x1»:

Листинг 2. Атрибуты трека 1.

```
[Entry 3]          ; данные элемента TOC №3
Session=1          ; элемент сессии 1
Point=0x01         ; данные трека 1 сессии 1
ADR=0x01           ; q-Mode == 1
Control=0x04       ; диск с данными, запрещенный
                   ; для копирования
TrackNo=0          ; трек, который мы сейчас читаем, -
                   ; это Lead-in-трек (т.е. TOC)
AMin=0             ; \
ASec=0             ;  + - абсолютный адрес текущего трека
AFrame=0           ; /
ALBA=-150          ; LBA-адрес текущего трека
Zero=0             ; это поле должно быть равно нулю,
                   ; как оно и есть
PMin=0             ; \
PSec=2             ;  + - абсолютный адрес начала трека 1
                   ;      сессии 1
PFrame=0           ; /
PLBA=0             ; LBA-адрес начала трека 1 сессии 1
```

Как мы видим, здесь присутствует как абсолютный, измеряемый в минутах, секундах, фреймах, так и LBA-адрес трека, представляющий собой не что иное, как порядковый номер сектора, считая от нуля. На самом деле, LBA-адрес – это «отсебятина», добавляемая в файл самим Clone CD, и в TOC LBA-адрес не хранится. Судя по всему, Clone CD вычисляет LBA-адрес исходя из соображений удобства (работать с LBA-адресацией действительно намного комфортнее). Однако при внесении каких-либо изменений в CCD-файл за согласованием обоих типов адресов нам придется следить самостоятельно. Для перевода абсолютных адресов в LBA можно воспользоваться следующей формулой:

```
Logical Sector Address=(((Minute*60)+Seconds)*75+Frame)-150
```

Ниже представлен вид атрибутов трека 1 до и после искажения:

Листинг 3. Атрибуты трека 1 до искажений (слева) и после искажения (справа).

```
[Entry 3]                              [Entry 3]
Session=1                              Session=1
Point=0x01                             Point=0x01
ADR=0x01                               ADR=0x01
Control=0x04                           Control=0x04
TrackNo=0                              TrackNo=0
AMin=0                                 AMin=0
ASec=0                                 ASec=0
AFrame=0                               AFrame=0
ALBA=-150                              ALBA=-150
Zero=0                                 Zero=0
PMin=0                    -->          PMin=10
PSec=2                    -->          PSec=2
PFrame=0                  -->          PFrame=0
PLBA=0                    -->          PLBA=-1
```

На самом деле, коварный автор схитрил и вместо вычислений LBA-адреса сослался на тот факт, что его версия Clone CD всегда использует абсолютные адреса, а LBA игнорирует.

Выбор абсолютного адреса первого трека произвольный, но осуществленный с таким расчетом, чтобы искаженный адрес гарантированно вылетал за границы первой сессии, Lead-out-область которой находится по адресу 00:29:33 (см. элемент TOC №2).

Шаг четвертый

Теперь смонтируем искаженный образ диска на виртуальный привод, создаваемый программой Alcohol 120%, и посмотрим, что из этого получилось. Конечно, нет никакой уверенности в том, что виртуальный привод поведет себя как настоящий, но ведь и настоящие приводы на искаженных дисках ведут себя по-разному! Поэтому использовать Alcohol в качестве рабочего «макетника» вполне допустимо, тем более что это экономит уйму времени и болванок, ведь монтирование виртуального диска в отличие от «прожига» болванки осуществляется мгновенно, если, конечно, оно вообще осуществляется… Вплоть до версии 1.4.3 включительно – самой свежей версии на момент написания этих строк – Alcohol органически не переваривал искаженные образы дисков и отказывался их монтировать, апеллируя к недоступности образа файла: «Unable to mount image. File not accessible». Судя по всему, Alcohol понимает искаженный TOC слишком буквально, пытаясь отыскать в файле-образе то, чего там заведомо нет (трека, начинающегося с адреса 10:02:00 и заканчивающегося адресом 00:29:33 там нет точно!).

Какая жалость! Возможность монтирования дисковых образов с искаженным TOC позволила бы нам преодолевать защиту от копирования на любых пишущих приводах, а не только на тех, что поддерживают режим RAW DAO, – просто сбрасываем образ защищенного диска на болванку в виде обыкновенного файла и динамически монтируем его Alcohol по мере необходимости. Выходит, что на проверку Alcohol оказывается гораздо менее крут, чем это кажется!

Шаг пятый

В порядке эксперимента попробуем «прожечь» искаженный образ в режиме RAW SAO, в котором, как уже было сказано выше, корректная запись сессий с искаженным TOC невозможна. Для гарантированного исключения возможных побочных эффектов желательно использовать привод, не поддерживающий RAW DAO чисто физически (ну мало ли, вдруг копировщик в плане проявления чудес искусственного интеллекта автоматически перейдет на более подходящий режим записи, игнорируя наши установки).

Мастер записи образов копировщика Alcohol 120% выдает следующую информацию о записываемом образе:

Листинг 4. Сводная информация по записываемому образу, выдаваемая Alcohol. Обратите внимание на размеры и адрес первого трека первой сессии (они выделены другим цветом).

```
Тип:       Файл-образ Clone CD
Путь:      L:\
Имя:       Image.ccd
           Image.img
           Image.sub
Размер:    8.81 MB
Сессий:    2
Треков:    2

Сессия 01:
  Трек 01: Mode 1, Длина: -42942(8191.92 GB), Адрес: 045000
Сессия 02:
  Трек 02: Mode 1, Длина: 001715(3.3 MB), Адрес: 013458
```

Вот это номер! Если верить Alcohol, то длина первого трека составляет целых 8 Тб. Этот чудовищный объем не то что на CD на DVD-диск не влезет! На самом деле, длина треков в TOC нигде явным образом не хранится, но вычисляется как разница стартовых адресов двух смежных треков (если же сессия содержит всего один трек, в ход идет адрес Lead-out-области, примыкающий к треку). Искажение стартового адреса первого трека привело к тому, что разница стартовых адресов Lead-out-области и этого самого трека стала отрицательной. Действительно, 00:29:33 – 10:02:00 = 2058 – 45000 = – 42942, а если вспомнить, что LBA-адреса по стандарту выражаются 32-разрядными неотрицательными числами, становится понятно, как Alcohol получил такой неестественно огромный объем (отрицательные числа – это такие числа, чей старший бит взведен, отсюда – маленькое отрицательное число – это очень большое положительное). Расчеты показывают, что заявленное Alcohol значение в 8 Тб достигается лишь при использовании 43-битных переменных. Вот это да! Alcohol спроектирован с запасом на будущее (а в будущем нас, как известно, ждут диски с объемами от 30 и более гигабайт, для адресации которых 32 бит оказывается уже недостаточно, плюс еще необходимо учесть резерв, предназначенный для «отлова» отрицательных длин, образовавшихся в результате жестоких извращений с TOC, ведь Alcohol – это защищенный копировщик!)

И вот наступает волнующий момент – момент заливки искаженного образа на CD-R/CD-RW-диск (внимание! используя CD-RW-диск, вы должны отдавать себе отчет в том, что можете его безвозвратно потерять! Если ваш единственный пишущий привод откажется опознавать такой диск, очистка последнего окажется невозможной!). Благополучно проглотив искаженный образ, Alcohol, безо всяких препирательств со своей стороны зажигает огонек индикации за-

писи (если, конечно, на вашем приводе он есть) и приступает к делу. Проходит минута, другая… а индикатор прогресса по-прежнему остается на нуле. К исходу шестой минуты, когда пишущая головка достигает кромки диска, процесс записи аварийно прерывается приводом и Alcohol, издав грустное «бэмс», сигнализирует об аппаратной ошибке.

Просмотр «недорезанного» диска на приводах ASUS и NEC обнаруживает лишь первую сессию, а от второй не видно и следа. С приводом PHILIPS дела обстоят еще хуже – он вообще отказывается признавать засунутую в него штуку лазерным диском, и после непродолжительного скрежета своих механических внутренностей, сопровождаемых натужными завываниями перебирающего различные скорости мотора, индикатор «DISC IN» прощально гаснет. «Прощально» в том смысле, что с испорченной болванкой вам придется расстаться. Конечно, если это всего лишь дешевый CD-R, то туда ему и дорога, но потерять CD-RW жалко. К счастью, на NEC очистка диска протекает успешно, и, воодушевленные этим обстоятельством, мы продолжаем свои издевательства вновь.

Копировщик Clone CD ведет себя в этом отношении иначе. Во-первых, он оценивает длину искаженного трека в 4 294 868 664 Кб (см. листинг, приведенный ниже), что указывает на использование 32-разрядных переменных и вытекающую отсюда невозможность отличать положительные длины от отрицательных.

```
Листинг 5. Сводная информация по записываемому образу, выдаваемая Clone CD. Обратите внимание на размер первого трека первой сессии (он выделен другим цветом).

ИНФОРМАЦИЯ О ФАЙЛЕ-ОБРАЗЕ:

Число сессий: 2
Занято на диске: 34850 Кбайт
Секторов: 15173
Время: 03:22:23 (мин:сек:кадр)

ИНФОРМАЦИЯ О СЕССИИ 1:

Размер сессии: 4726 Кбайт
Число треков: 1
Pregap: Данные Mode 1, размер: 103359 Кбайт
Track 1: Данные Mode 1, размер: 4294868664 Кбайт

ИНФОРМАЦИЯ О СЕССИИ 2:

Размер сессии: 3939 Кбайт
Число треков: 1
Track 2: Данные Mode 1, размер: 3939 Кбайт
```

Во-вторых, обнаружив, что запись искаженного TOC на данном приводе невозможна, Clone CD корректирует TOC так, чтобы его облик принял человеческий вид. В результате процесс «прожига» протекает без каких-либо ошибок и мы получаем как будто бы работоспособный диск. Стартовый адрес первого трека начинается там, где кончается Lead-in-область первой сессии (точнее, pre-gap первого трека начинается там, где кончается post-gap Lead-in-области первой сессии, но это уже детали). Такой диск нормально читается в любом приводе CD-ROM, но! Если защитный механизм прочитает содержимое TOC, он легко обнаружит, что имеет дело с копией, но не с оригиналом. Спрашивается: и на кой черт нам такое копирование нужно?! Хоть бы предупреждение было какое… Ладно, профессионалы запросто определят, в чем подвох, но в каком положении окажутся новички, и/или просто квалифицированные пользователи, использующие Clone CD для своих нужд? В общем мрак, одним словом…

Правда, в режиме RAW DAO нарезка искаженного образа протекает отлично и Clone CD не вносит в TOC никакой отсебятины, благодаря чему у нас образуется действительно защищенный CD, который мы сейчас и будем ломать.

Шаг шестой

Просмотр защищенного диска под приводом NEC показывает все файлы, даже те, что принадлежат первому треку – тому самому треку, чей стартовый адрес жестоко искажен. Двойной щелчок мышью доказывает, что файлы не только присутствуют в каталоге, но и успешно открываются ассоциированным с ними приложениям и, судя по всему, выглядят вполне нормальными. Нашу душу начинают грызть смутные сомнения: действительно ли пишущий привод записал стартовый адрес первого трека таким, каким мы просили, или молчаливо исправил его на лету?

Для ответа на этот вопрос мы должны исследовать геометрию диска, т.е., попросту говоря, прочитать TOC. Запускаем уже полюбившийся нам Roxio Easy CD Creator и в меню «CD» находим пункт «CD Information». Щелкаем по нему мышкой, и на экран тут же выпрыгивает диалоговое окно с раскладкой диска (внимание! не все программы способны «переваривать» искаженный TOC! Easy CD Creator это умеет, а вот, например, Record NOW! – нет. В отсутствии подходящей утилиты вы можете воспользоваться программой raw.TOC.exe, поставляемой вместе с этой книгой).

Как и следовало ожидать, стартовый адрес первого трека лежит далеко за пределами своей «родной» сессии, и его длина, будучи выраженная положительным числом, значительно превышает доступную емкость диска (см. рис. ниже). Так что все наши волнения абсолютно безосновательны!

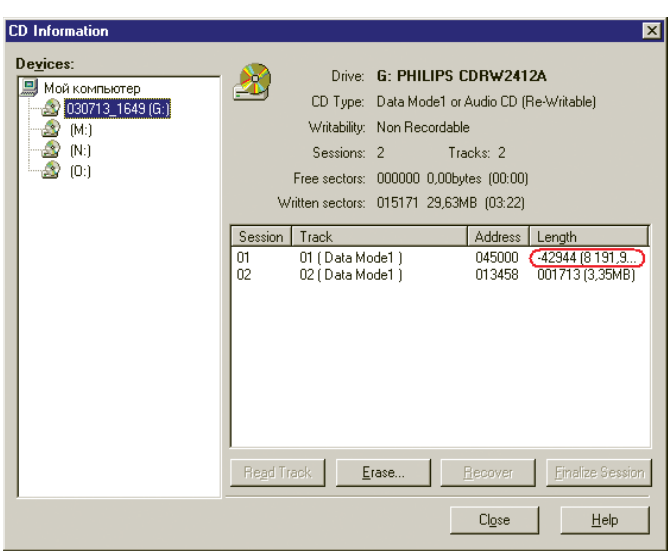

Рисунок 1. Отрицательная длина первого трека сводит штатный копировщик с ума

Постойте, но как же тогда осуществляется доступ к содержимому первого трека? А кто вам вообще сказал, что лазерный диск адресуется по трекам?! Основной адресацией лазерного диска с данными является сектор. Абсолютный же адрес всякого сектора однозначно определяется принадлежащим ему Q-каналом подкода (с учетом не-

совпадения границ секций и секторов максимально возможное расхождение, допускаемое стандартом, составляет 1 сек, т.е. 75 секторов, поэтому этот способ используется лишь для грубого позиционирования оптической головки). Точная наводка на цель выполняется непосредственно по самому секторному заголовку, в явном виде содержащему его абсолютный адрес. Номера треков в процессе обработки сектора вообще не участвуют, вернее могут и не участвовать… Но могут ведь и участвовать! Все зависит от электронной начинки привода и его микропрограммной прошивки. Как именно они в этом участвуют – сие есть великая тайна разработчиков привода, и простым смертным ее понять не дано. Но так или иначе, встретив некорректный TOC, некоторые приводы запутываются, и в стройных битовых рядах возникает настоящая сумятица.

Результаты тестирования трех моих приводов следующие: NEC, как уже говорилось выше, показывает содержимое обоих секций, корректно обрабатывая их содержимое. ASUS показывает только первую – искаженную – сессию и в упор не видит вторую, делая ее недоступной даже на секторном уровне. Зато файлы первой сессии обрабатываются вполне корректно. PHILIPS, напротив, видит обе сессии, но корректно обрабатывает файлы лишь последней из них (т.е. той, что не искажена). Искаженная сессия доступна на секторном уровне, но нестабильно. Иногда без всяких видимых причин PHILIPS и возвращает лишенный всякого смысла мусор.

Мораль: защитные механизмы, базирующиеся на искаженном TOC, не могут закладываться ни на одну из сессий. Поэтому обе сессии должны дублировать содержимое друг друга – авось хоть одну из них привод пользователя да прочтет. Какой же тогда в этой защите смысл? А вот какой – пускай защита не может без риска для жизни привязаться к сессиям, она может привязаться к сырому содержимому TOC. О том, как осуществить такую привязку на практике, мы поговорим чуточку позднее, а пока попробуем скопировать защищенный диск нашими фаворитами – Clone CD и Alcohol 120%.

Автоматическое копирование и обсуждение его результатов

В какой бы привод защищенный диск ни был вставлен, Clone CD выдает неизменно постоянный результат, не имеющий ничего общего с реальной действительностью. По его скромному мнению, диск содержит всего одну сессию с общей протяженностью в 4,6 Мб, но зато размер единственного трека последней составляет ни много ни мало – 3,9 Тб!

Листинг 6. Таким видит защищенный диск копировщик Clone CD. Обратите внимание, что он распознал лишь одну сессию из двух (первую), да и то неправильно.

```
ИНФОРМАЦИЯ О CD В ДИСКОВОДЕ:
Число сессий: 1
Занято на диске: 4726 Кбайт
Секторов: 2058
Время: 00:27:33 (мин:сек:кадр)

ИНФОРМАЦИЯ О СЕССИИ 1:

Размер сессии: 4726 Кбайт
Число треков: 1
Pregap: Данные Mode 1, размер: 103359 Кбайт
Track 1: Data, размер: 4294868664 Кбайт
```

Еще до завершения процесса копирования нас начинают одолевать стойкие сомнения или, я бы даже сказал, непоколебимая уверенность в том, что диск будет скопирован неправильно. И действительно, чего мы опасались, то мы и получили! Давайте создадим образ скопированного диска в плане сравнения копии TOC с оригиналом.

Листинг 7. Образ защищенного диска, снятый программой Clone CD (несоответствующие поля выделены другим цветом).

```
[CloneCD]                ; данные о копировщике
Version=3                ; версия Clone CD

[Disc]                   ; данные о диске
TocEntries=7             ; количество элементов TOC = 7
                         ; (в оригинале было 12)
Sessions=1               ; кол-во сессий = 1
                         ; (в оригинале было 2)
DataTracksScrambled=0    ; поле DVD
CDTextLength=0           ; CD-Text в полях подкода
                         ; Lead-in-области отсутствует
[Session 1]         ; данные сессии 1
PreGapMode=1        ; тип трека == Mode 1
PreGapSubC=0        ; данных подканала - нет

[Entry 0]           ; данные элемента TOC №0
Session=1           ; элемент сессии 1
Point=0xa0          ; номер первого трека сессии 1
                    ; в PMin/тип диска в PSec
ADR=0x01            ; q-Mode == 1
Control=0x04        ; диск с данными, запрещенный
                    ; для копирования
TrackNo=0           ; трек, который мы сейчас читаем, -
                    ; это Lead-in-трек (т.е. TOC)
AMin=0              ; \
ASec=0              ;  + - абсолютный адрес текущего трека
AFrame=0            ; /
ALBA=-150           ; LBA-адрес текущего трека
Zero=0              ; это поле должно быть равно нулю,
                    ; как оно и есть
PMin=1              ; номер первого трека сессии 1
PSec=0              ; тип диска CD-DA и CD-ROM-диск в Mode 1
PFrame=0            ; не несет никакой полезной информации
PLBA=4350           ; номер трека, представленный Clone CD
                    ; как LBA-адрес, т.е. глупость
[Entry 1]           ; данные элемента TOC №1
Session=1           ; элемент сессии 1
Point=0xa1          ; номер последнего трека сессии 1 в PMin
ADR=0x01            ; q-Mode == 1
Control=0x04        ; диск с данными, запрещенный
                    ; для копирования
TrackNo=0           ; трек, который мы сейчас читаем, -
                    ; это Lead-in-трек (т.е. TOC)
AMin=0              ; \
ASec=0              ;  + - абсолютный адрес текущего трека
AFrame=0            ; /
ALBA=-150           ; LBA-адрес текущего трека
Zero=0              ; это поле должно быть равно нулю,
                    ; как оно и есть
PMin=1              ; номер последнего трека сессии 1
                    ; (в сессии только один трек)
PSec=0              ; не несет никакой полезной информации
PFrame=0            ; не несет никакой полезной информации
PLBA=4350           ; номер трека, представленный Clone CD
                    ; как LBA-адрес, т.е. глупость
[Entry 2]           ; данные элемента TOC №2
Session=1           ; элемент сессии 1
Point=0xa2          ; положение Lead-out-области
                    ; в PMin:PSec:PFrame
ADR=0x01            ; q-Mode == 1
Control=0x04        ; диск с данными, запрещенный
                    ; для копирования
TrackNo=0           ; трек, который мы сейчас читаем, -
                    ; это Lead-in-трек (т.е. TOC)
AMin=0              ; \
ASec=0              ;  + - абсолютный адрес текущего трека
AFrame=0            ; /
ALBA=-150           ; LBA-адрес текущего трека
Zero=0              ; это поле должно быть равно нулю,
                    ; как оно и есть
PMin=0              ; \
PSec=29             ;  + - абсолютный адрес Lead-out-области
                    ;      сессии 1
PFrame=33           ; /
PLBA=2058           ; LBA-адрес Lead-out-области сессии 1
```

```
[Entry 3]          ; данные элемента TOC №3
Session=1          ; элемент сессии 1
Point=0x01         ; данные трека 1 сессии 1
ADR=0x01           ; q-Mode == 1
Control=0x04       ; диск с данными, запрещенный
                   ; для копирования
TrackNo=0          ; трек, который мы сейчас читаем, -
                   ; это Lead-in-трек (т.е. TOC)
AMin=0             ; \
ASec=0             ;  + - абсолютный адрес текущего трека
AFrame=0           ; /
ALBA=-150          ; LBA-адрес текущего трека
Zero=0             ; это поле должно быть равно нулю,
                   ; как оно и есть
PMin=10            ; \
PSec=2             ;  + - абсолютный адрес начала трека 1
                   ;      сессии 1
PFrame=0           ; /
PLBA=45000         ; LBA-адрес начала трека 1 сессии 1

[Entry 4]          ; данные элемента TOC №4
Session=1          ; элемент сессии 1
Point=0xb0         ; позиция следующей записываемой области
                   ; в AMin:ASec:AFrame
ADR=0x05           ; q-Mode == 1
Control=0x04       ; диск с данными, запрещенный
                   ; для копирования
TrackNo=0          ; трек, который мы сейчас читаем, -
                   ; это Lead-in-трек (т.е. TOC)
AMin=2             ; \
ASec=59            ;  + - абсолютный адрес следующей
                   ;      записываемой области
AFrame=33          ; /
ALBA=13308         ; LBA-адрес следующей записываемой области
Zero=3             ; количество pointer в Mode 5
PMin=22            ; \
PSec=14            ;  + - абсолютный адрес максимальной
                   ;      записываемой области
PFrame=34          ; /
PLBA=99934         ; LBA-адрес максимальной записываемой
                   ; области
[Entry 5]          ; данные элемента TOC №5
Session=1          ; элемент сессии 1
Point=0xc0         ; стартовый адрес Lead-in-области
                   ; Hybrid-диска (если он есть)
ADR=0x05           ; Mode 5 (Оранжевая книга)
Control=0x04       ; диск с данными, запрещенный
                   ; для копирования
TrackNo=0          ; трек, который мы сейчас читаем, -
                   ; это Lead-in-трек (т.е. TOC)
AMin=162           ; рекомендуемая мощность лазера для
ASec=200           ; Application code (в оригинале здесь
                   ; было 128)
AFrame=224         ; в оригинале здесь было 140
ALBA=294074        ; LBA-"адрес" трех предыдущих полей
Zero=0             ; зарезервировано
PMin=97            ; \
PSec=27            ;  + - абсолютный адрес Lead-in-области
                   ;      Hybrid-диска
PFrame=21          ; / (адрес лежит за пределами диска,
                   ; т.е. Hybrid-диска нет)
PLBA=-11604        ; LBA-адрес Lead-in-области Hybrid
                   ; (вычислен с переполнением)
[Entry 6]          ; данные элемента TOC №6
Session=1          ; элемент сессии 1
Point=0xc1         ; копия ATIP-информации
ADR=0x05           ; -+
Control=0x04       ; -+
TrackNo=0          ; -+
AMin=4             ; -+
ASec=192           ; -+
AFrame=150         ; -+- ATIP (изменена!)
ALBA=32400         ; -+
Zero=0             ; -+
PMin=0             ; -+
PSec=0             ; -+
PFrame=0           ; -+
PLBA=-150

[TRACK 1]
MODE=0
INDEX 1=45000
```

Сокращение сессий с двух до одной очень сильно смущает. Куда девалась вторая – неискаженная(!) сессия, вообще непонятно. И, хотя искаженные данные первого трека сохранились, оказались неожиданно измененными поля Application Code и ATIP (и это несмотря на то, что запись производилась на ту же самую CD-RW-болванку, что и раньше, хотя ее «прожиг» осуществлялся различными приводами).

Как следствие: скопированный диск оказывается работоспособен не на всех приводах (ASUS и NEC его прочитают, а вот PHILIPS – нет), к тому же защите ничего не стоит прочитать текущий TOC и сравнить его с эталонным.

Короче говоря, «факир был пьян, и фокус не удался». Что ж, попробуем обратиться за помощью к Alcohol– уж он-то должен наверняка с этим справиться. Действительно, Alcohol видит обе сессии: как искаженную, так и неискаженную, однако по малопонятным причинам сохраняет в образ лишь вторую из них (Clone CD сохранял первую). Ну что это за зоопарк, а? Содержимое TOC скопированного диска можно даже и не сравнивать – там будет далеко не то, что защита собирается ожидать. И напрасно! Содержимое TOC, снятое Alcohol, практически полностью соответствует оригиналу. Единственно, в чем ошибся Alcohol, – определил тип pre-gap обоих треков не как Mode 1, но как Mode 2. Впрочем, в силу отсутствия в образе первой сессии полученная с его помощью копия диска все равно оказывается неработоспособной.

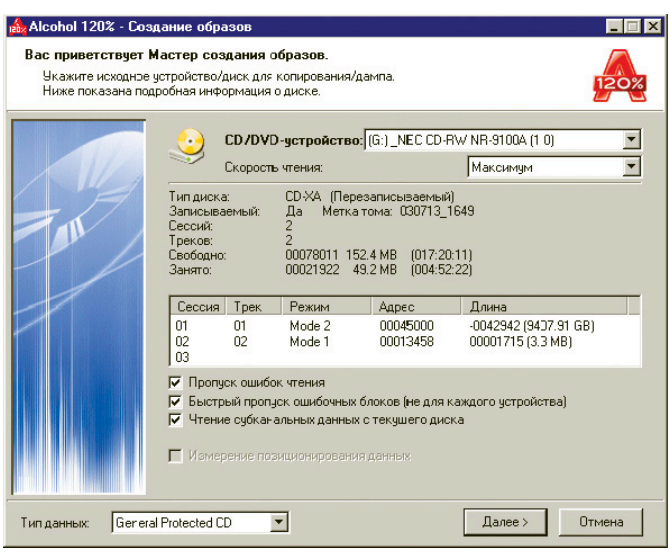

Рисунок 2. Alcohol видит обе сессии защищенного диска, но…

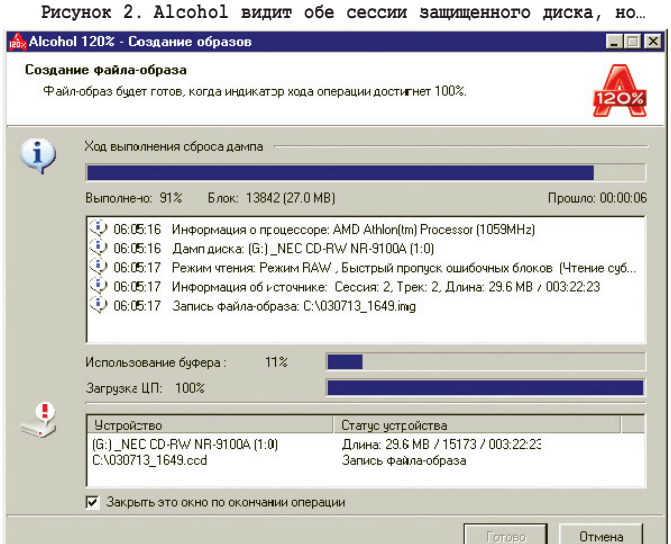

Рисунок 3. Копирует лишь вторую из них, а первую нагло пропускает

А ведь заявлялось, что Clone CD/Alcohol 120% способны копировать любые существующие на сегодняшний момент защищенные диски, и вдруг на поверку оказывается, что даже такую простую защиту, которую может создать на кончике пенька любой программист, они преодолеть ни вместе, ни по раздельности не в состоянии! Причем аппаратура, на которой все эти эксперименты и осуществлялись, возможность корректного копирования искаженного диска гарантированно поддерживает (сам проверял), и потому отмахнуться физическими ограничениями приводов разработчикам обоих копировщиков уже не удастся!

Даже не верится, что такой простой прием «ослепляет» лучших копировщиков защищенных дисков! Неужели и вправду создание некопируемых дисков вполне осуществимо на обыкновенном бытовом оборудовании?! Да! Именно так! Конечно, не стоит путать некопируемость диска автоматическими копировщиками с принципиальной невозможностью получения его идентичной копии. В ручном режиме копирование таких дисков вполне осуществимо (правда, при условии, что ваш пишущий привод поддерживает режим RAW DAO, а читающий – читает сектора из обоих секций), и сейчас мы продемонстрируем как.

Так как же все-таки скопировать такой диск?

Конечно, с помощью «Добермана Пинчера» (или любого другого блочного копировщика файлов), HIEW, двух образов защищенного диска (один – с первой сессией – от Clone CD, другой – со второй сессией – от Alcohol) мы можем воссоздать идентичную копию оригинального диска путем их совокупного объединения, но… это будет както не по-хакерски, да и вообще некрасиво.

Чтобы не писать свою собственную программу «прожига» диска, ограничимся использованием Clone CD. При условии, что подсунутый ему образ диска запечатлен правильно, Clone CD обычно справляется с прожигом «на ура». Итак, у нас есть более и менее верный файл image.ccd, содержащий TOC, но недостает файла образа image.img. Попробуем его получить? Будем отталкиваться от того, что LBA-адреса всех секторов диска пронумерованы последовательно, включая области, занятые Lead-In/Lead-Out и прочим служебным барахлом. Разумеется, непосредственное чтение служебных областей диска на секторном уровне невозможно, но… именно на этом мы и собираемся сыграть! Последовательно читая диск с первого по последний сектор, мы обнаружим, что сектора с LBA-адресами с 0 по 2055 сектор включительно читаются без каких-либо проблем, после чего наступает сумеречная зона нечитающихся секторов, протянувшаяся вплоть до сектора 13307. Здесь сектора либо совсем не читаются либо возвращаются в сильно мутированном виде, легко опознаваемые по отсутствию правильной синхропоследовательности в их заголовке. Наконец, с адреса 13308 чтение вновь продолжается без каких-либо проблем.

Судя по всему мы имеем дело с двухсессионным диском и сумеречная зона между сессиями есть ни что иное, как Lead-Out/Lead-In. Накинув два сектора на post-gap (при условии, что он записан с соблюдением стандарта), получаем, что LBA-адрес последнего значимого сектора первой сессии составляет 2057 или, в пересчете на абсолютные единицы – 00 минут, 29 секунд и еще 32 фрейма. Соответственно, LBA-адрес первого сектора второй сессии равен 13308 + 150 (pre-gap) == 13458, или 3 минуты, 1 секунда, 33 фрейма. Конечно, если исследуемый диск содержит большое количество ошибок, то его анализ значительно усложняется, т.к. физические дефекты на секторном уровне могут выглядеть точно так же, как Lead-In/Lead-Out-области, конечно, при том условии, что дефективные области имеют соответствующую протяженность, – а это вряд ли.

Отбросив сектора, расположенные в зонах pre- и post-gap (т.е. 150 секторов от конца первой читаемой области и ровно столько же от начала следующей), мы должны объединить их в один файл, используя для этой цели любой файловый копировщик (например, штатную команду MS-DOS copy file_1 /b + file_2 image.img). Остается прочитать сырой TOC SCSI/ATAPI командой READ TOC (opcode: 43h, format: 2h) и записать его в image.ccd файл в соответствии с синтаксисом Clone CD. Как альтернативный вариант – можно воспользоваться ccd-файлом, сформированным программой Alcohol, предварительно скорректировав pregap Mode (как уже сказано выше, Alcohol определил его неправильно, перепутав Mode 1 с Mode 2). Согласно стандарту режим сектора задается пятнадцатым, считая от нуля, байтом его заголовка. Если этот байт равен одному (что, собственно, и наблюдается в нашем случае), то и Mode сектора будет 1, но не 2.

При условии, что все сделано правильно, после записи собственноручно сформированного образа диска мы получаем практически идентичный оригинал. Просто? Да проще простого! И написать автоматический копировщик, автоматизирующий наш труд, можно буквально за несколько часов! Если чтение «сырых» секторов с диска представляет для вас проблему, воспользуйтесь исходными текстами утилит ASPI32.raw/SPTI.raw, как раз такое чтение и осуществляющих.

Так что искажение TOC – не очень-то надежный прием защиты от копирования, как ни крути. Правда, от обычных пользователей, вооруженных Clone CD/Alcohol, он все-таки спасает, а больше от защиты зачастую и не требуется.

Пример реализации защиты на программном уровне

Покажем теперь, как такая защита может быть реализована на программном уровне. Самое простое, что можно сделать, – отправить приводу команду «сырого» чтения TOC (opcode: 43h, format: 2h) и сравнить возвращенный ею результат с эталоном. Какие именно поля TOC защита будет проверять, – это ее личное дело. По минимуму достаточно проверить количество сессий и стартовый адрес искаженного трека. По максимуму можно контролировать весь TOC целиком. Естественно, от побайтового сравнения контролируемого TOC с оригиналом настоятельно рекомендуется воздержаться, т.к. это неявно закладывает защиту на особенности микропрограммной прошивки читающего привода. Стандарт ничего не говорит о том, в каком порядке должно возвращаться содержимое TOC, и потому его бинарное представление может варьировать-

ся от привода к приводу. Грамотно спроектированная защита должна анализировать только те поля, к содержимому которых она привязывается явно.

Демонстрационный пример, приведенный ниже, как раз и иллюстрирует технику корректной привязки к TOC. Разумеется, явная проверка целости TOC может быть элементарно обнаружена хакером и выкинута из программы как ненужная, поэтому не стоит копировать этот демонстрационный пример один к одному в свои программы. Лучше используйте значения полей TOC как рабочие константы, жизненно необходимые для нормальной работоспособности программы, – в этом случае сличение паспортов с лицами будет не столь наглядным. Естественно, явная проверка оригинальности диска все равно обязана быть, но ее основная цель отнюдь не защитить программу от взлома, а довести до сведения пользователя, что проверяемый диск с точки зрения защиты не является лицензионным.

Листинг 8. Демонстрационный пример простейшей защиты, привязывающейся к искаженному TOC и не позволяющей себя копировать.

```
/*-------------------------------------------------------
 *
 *                       crack me 9822C095h
 *                       ==================
 *
 * демонстрация техники привязки к искаженному TOC;
 * для работе программе требуется лазерный диск, прожженный
 * соответствующим образом
-------------------------------------------------------*/
#include <stdio.h>
#include <windows.h>
#include "CD.h"
#include "SPTI.h"
#include "ASPI32.h"

// параметры защищенного диска, которые мы будем проверять
//-------------------------------------------------------
#define _N_SESSION    2          // количество сессий
#define _TRACK        1          // номер проверяемого трека
#define _TRACK_LBA    0x6B124    // стартовый LBA-адрес
                                 // трека _TRACK

// параметры программы
//--------------------
#define MAX_TRY        3  // мак. кол-во попыток чтения TOC
#define TRY_DELAY      100       // задержка между попытками
#define MAX_TOC_SIZE  (2352)     // максимальный размер TOC


main(int argc, char **argv)
{
    // основные переменные
    long a, real_len, try = 1;
    // сюда будет читаться TOC
    unsigned char TOC[MAX_TOC_SIZE];
    // SCSI CDB-блок для SCSI/ATAPI-устройств
    unsigned char CDB[ATAPI_CDB_SIZE];

    // TITLE
    fprintf(stderr,"crackme 9822C095 by Kris Kaspersky\n");

    if (argc <2)
    {
           fprintf(stderr,"USAGE:crackme.9822C095h.exe ↵
                  drive\n");
           fprintf(stderr,"\tdrive - \\\\.\\X: or ↵
                  Trg.Lun\n");
           return -1;
    }

    // инициализация буферов
    memset(CDB, 0, ATAPI_CDB_SIZE); memset(TOC, 0, ↵
           MAX_TOC_SIZE);

    // готовим CDB-блок
    CDB[0] = 0x43;               // READ TOC
    CDB[2] = 0x2;                // RAW TOC
    CDB[6] = 0;                  // номер первой сессии
    CDB[7] = HIBYTE(MAX_TOC_SIZE);      // размер...
    CDB[8] = LOBYTE(MAX_TOC_SIZE);      // ...буфера

    // читаем TOC
    while(1)
    {
           // посылаем CDB-блок SCSI/ATAPI-устройству
           a = SEND_SCSI_CMD(argv[1], CDB, ATAPI_CDB_SIZE, ↵
                  NO_SENSE, TOC, MAX_TOC_SIZE, SCSI_DATA_IN);
           // TOC успешно прочитан, рвем когти
           if (a == SCSI_OK) break;

           // произошла ошибка. Возможно привод не готов?
           // выдерживаем паузу
           Sleep(TRY_DELAY);
           // максимальное количество попыток уже вышло?
           if (try++ == MAX_TRY)
                  { fprintf(stderr,"-ERR: can not read ↵
                         TOC\x7\n"); return -1;}
    }

    // TOC прочитан, приступаем к его анализу
    //---------------------------------------

    // проверка количества сессий
    if ((TOC[3] - TOC[2]) != (_N_SESSION-1))
                  {fprintf(stderr, "-ERR: not original ↵
                         CD\n");return -1;}

    // проверка стартового LBA-адреса трека _TRACK
    //--------------------------------------------
    // определение реальной длины TOC
    real_len = TOC[0]*0x100L+TOC[1];
    // перебор всех entry
    for (a = 4; a < real_len; a+=11)
    {
           // это наш трек?
           if (TOC[a+3] == _TRACK)
                  if ((((TOC[a + 4]*60L) + TOC[a + 5])*75L) + ↵
                         TOC[a + 6] != _TRACK_LBA)
                         {fprintf(stderr, "-ERR: ↵
                                not original LBA\n"); ↵
                                return -1;}
           else
                  break;
    }

    // это оригинальный диск!
    printf("Hello, original CD\n");
}
```

Предлагаемая защита не копируется Clone CD (т.к. он создает всего одну сессию вместо ожидаемых двух), но легко обходится Alcohol, который хоть и помещает на место первой секции непотребный мусор, зато вполне корректно воссоздает оригинальный TOC.

Для усиления защиты мы можем попытаться не только проверять обе сессии на существование, но и контролировать целостность их содержимого. Разумеется, не обязательно перелопачивать каждую из секций целиком. Достаточно выбрать несколько ключевых секторов, желательно имеющих по возможности уникальное содержимое. Постойте! – воскликнет внимательный читатель. Разве автор не предостерегал нас о последствиях такой проверки?! Ведь никто не может гарантировать, что на оборудовании пользователя эти сектора вообще прочтутся! Что ж, отвечу я. Закладываться на читабельность секторов действительно категорически не рекомендуется, но вот контролировать успешно просчитавшиеся сектора можно и нужно! То есть: если ключевые сектора не читаются, то все ок и нет никаких поводов считать диск нелицензионным – это просто у конечного пользователя оборудование такое (в смысле кривое). Другое дело, если чтение секторов прошло без ошибок, но вместо ключевых данных в них оказалось нечто совсем иное. Вот тогда, действительно, проблема не в оборудовании, а в диске.

Усиленный вариант защиты уже не копируется Alcohol (т.к. вместо оригинального содержимого первой сессии Alcohol помещает на диск какой-то дикий мусор), но может быть скопирован вручную по методике, описанной выше. К тому же, привязка к искаженному TOC элементарно отламывается в отладчике/дизассемблере. Так что дальнейшее совершенствование защиты практически полностью бессмысленно. От «простых смертных» пользователей мы уже защитились, а от хакеров мы не сумеем защититься все равно (во всяком случае, не этим способом). В любом случае более продвинутые защиты – тема отдельного разговора.

[1] Посмотрите внимательно на лицевую панель своего CD-ROM, видите – внизу лотка расположено крохотное отверстие порядка 1 мм в диаметре? Воспользовавшись любым длинным тонким и достаточно прочным предметом, например, металлической канцелярской скрепкой, слегка приоткройте лоток, введя «отмычку» в указанную дырку до упора и еще чуть-чуть надавив. Все! – дальше лоток можно выдвинуть уже руками. Внимание! Во-первых, проделывайте эту операцию только при выключенном компьютере, а во-вторых, держите «отмычку» строго горизонтально, иначе вы можете промазать и угодить в какой-нибудь нежный узел, основательно его повредив.

Условные обозначения

- Под приводом NEC понимается _NEC CD-RW NR-9100A; firmware version 1.4.
- Под приводом ASUS понимается ASUS CD-S500/A; firmware version 1.4K.
- Под приводом PHILIPS понимается PHILIPS CDRW2412A; firmware version P1.55.

Alcohol 120% – отличный копировщик защищенных дисков, условно-бесплатную версию которого можно утянуть с сайта http://www.alcohol-soft.com/. Автоматически ломает более половины всех существующих типов защит от копирования и позволяет динамически монтировать образы защищенных дисков на виртуальный привод CD-ROM, что очень удобно для экспериментов. К сожалению, монтированию подлежат лишь «правильные» образы, коими большинство образов защищенных дисков отнюдь не являются.

Clone CD – хороший копировщик защищенных дисков, условно-бесплатную версию которого можно утянуть по следующему адресу: http://www.elby.ch/. С копированием защищенных дисков в полностью автоматическом режиме Clone CD справляется скорее плохо, чем хорошо, однако после ручного шаманства с настройками и непосредственно самим образом защищенного диска он может скопировать добрую половину существующих типов защит. Утверждение о том, что Clone CD «берет» практически все существующие защиты от копирования, – ложное и невероятно далеко от действительности.

Глоссарий

Lead-In Area – вводная область диска. Служебная область диска, по сути своей представляющая нулевой трек, всегда предшествующий первому треку PA. Каждая сессия многосессионного диска имеет собственную вводную область. Размер вводной области по стандарту составляет 9 мегабайт (60 секунд, или 4500 секторов). Q-канал подкода вводной сессии содержит TOC, среди прочей полезной информации, указывающей либо на адрес выводной области (закрытый диск), либо на адрес вводной области следующей сессии (открытый диск). Содержимое вводной области недоступно для чтения на программном уровне. Визуально вводная область выглядит равномерно освещенным блестящим кольцом.

Lead-Out Area – выводная область диска. Служебная область диска, условно обозначаемая треком номер AAh и замыкающая собой всякую закрытую сессию. Выводная область служит своеобразным индикатором конца сессии и/или диска и помогает оптической головке не вылететь за пределы диска. Пишущие приводы должны корректно обрабатывать диски с незакрытыми сессиями, однако обыкновенные приводы CD-ROM и аудиопроигрыватели это делать не обязаны. Внимание! Отсутствие выводной сессии (равно как и некорректное задание ее адреса) может повредить некоторые модели приводов (один из них PHILIPS).

Емкость выводной области односессионного диска по стандарту составляет 13,5 Мб (6750 секторов или 1,5 минуты). Емкость выводных областей для второй и последующих сессий многосессионных дисков уменьшена до 4 Мб (0,5 минуты, или 2250 секторов). Содержимое выводной области недоступно на программном уровне. Визуально выводная область выглядит равномерно освещенным блестящим кольцом.

Program Area – программная область. Область диска, расположенная между Lead-In- и Lead-Out-областями и содержащая информационные треки с музыкой или данными. Это – основная область диска, целиком доступная на секторном уровне с паузами между аудиотреками включительно.

TOC – (Table Of Content) – таблица содержимого или попросту оглавление диска. Служебная область диска, записанная в Q-канале подкода вводной области диска, также называемой Lead-In-областью (такое блестящее кольцо у внутреннего края диска). Многосессионный диск имеет несколько независимых TOC – по одному TOC на каждую закрытую сессию.

TOC содержит информацию о стартовых адресах вводной/выводной областей диска и атрибуты всех его треков (как-то тип трека: аудио или данные, а если данные, то в каком режиме – Mode 1, Mode 2 и т. д., абсолютный стартовый адрес трека и номер соответствующей ему сессии). Также TOC содержит часть ATIP и указатели на местоположение ее продолжения.

Непосредственно (т.е. на секторном уровне) для чтения TOC недоступен, но для извлечения его содержимого в «сыром» виде можно воспользоваться следующей SCSI/ATAPI командой READ TOC/PMA/ATIP (операционный код: 43h) с format field == 2h.

Однако не стоит путать TOC с файловой системой – между ними нет ничего общего! Файловые системы на лазерных дисках хранятся непосредственно в PM и свободно доступны для чтения на секторном уровне.