Скрытый потенциал

Модификация прошивок DVD-рекордеров

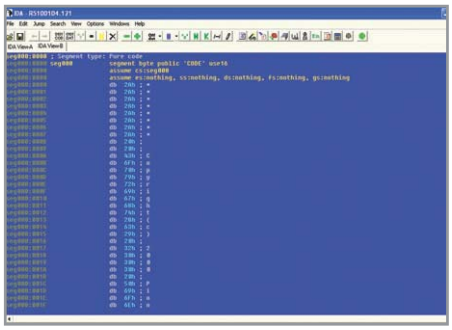
Современная инженерия закладывает в свои детища потенциал, о котором конечный пользователь даже может и не подозревать. Говоря о DVD-рекордерах, можно отметить, что порой достаточно всего лишь сменить прошивку, чтобы добиться просто потрясающих результатов.

Сначала вкратце расскажем о специфике прошивок в DVD-рекордерах. В общем и целом задача прошивки привода — быть связующим звеном между аппаратной и программной частями. В данном случае воспринимать прошивку нужно как флэш-память, в которой записаны команды-инструкции, выполняемые приводом в ответ на определенные произошедшие или происходящие события. Таким событием может быть и нажатие кнопки «Eject», и определение вставленного диска.

Обычно меняют прошивку по нескольким причинам. Первая из них — это ликвидация заводских «багов»: устраняются сбои, происходящие при взаимодействии с некоторыми программными или аппаратными составляющими компьютера. Для такого случая лучше воспользоваться обновленной прошивкой, которая регулярно появляется на сайте фирмы-производителя, сделавшей ваш привод. Следующей весомой причиной, способной подтолкнуть к замене прошивки, является придание аппарату новых функциональных возможностей.

Если же говорить о неофициальной перепрошивке DVD-приводов и рекордеров, здесь можно вывести примерно следующую пропорцию: 80% таких операций проводится для снятия защиты на регион для видео DVD, о чем, мы полагаем, многие из вас знают. Остальные 20% приходится на «разгонные» модификации, но они чаще всего являются случайным бонусом, появившимся в результате разблокировки региона. В частности, у некоторых DVD-рекордеров такими модифицированными прошивками можно развить способность читать и записывать диски быстрее. В случае с чтением имеется в виду, например, такой интересный момент, как списывание DVD-видеодисков. Некоторые производители рекордеров и приводов специально закладывают ограничения по скорости работы с такими дисками, чтобы отбить охоту у желающих переписать или перекодировать лицензионный фильм. Кроме того, в прошивках DVD-устройств содержатся »

» идентификационные данные о болванках, с которыми привод совместим, и информация о том, как именно нужно работать с болванкой определенной серии того или иного производителя. Основной плюс такой перепрошивки заключается в том, что большинство официально не сертифицированных дисков можно записывать на более высокой скорости. Единственный побочный эффект, как и при всяком разгоне, это нестабильность. В данном случае нестабильность записи ведет к тому, что данные на диске могут плохо считываться. Теоретически для каждой такой идентификационной записи можно создать уникальную модель поведения, удовлетворяющую требованиям конкретного пользователя. И все бы ничего, но жестокая реальность в лице компаний-производителей заметно осложняет этот процесс.



▲ Чтобы редактировать прошивку, надо быть хорошим программистом

▲ Первый привод из линейки Pioneer, научившийся записывать на 2x

Минус раз, минус два

Толчком к появлению различных прошивок, созданных в первую очередь энтузиастами разгона, стала сложная ситуация, сложившаяся со стандартами записываемых дисков. Дело в том, что даже на сегодняшний момент как стандарт определены диски для однократной записи, способные записываться только на скоростях 1x и 4x. Между этими двумя жестко ограниченными скоростными показателями смог протиснуться еще один, полуофициальный режим записи — 2x. Именно его появление и обуславливает возможный «разгон» записывающего привода. Его же появление повлекло за собой ряд странных, необъяснимых скоростных ограничений, касающихся как болванок, так и рекордеров.

Технология 2x является «коронным номером» компании Pioneer, которая уже давно и успешно работает на этом рынке. Серийно эта технология стала применяться начиная с модели A03.

Такого результата компания добилась за счет своих собственных разработок, и она до сих пор является фактически монополистом. Для того чтобы объяснить принцип записи на 2x, введем понятие «стратегия записи». Стратегия записи — это участок кода, находящийся в прошивке привода или в идентификационном коде болванки, содержащий ряд технических параметров, которые привод должен учесть при обработке диска. В стратегии записи указываются данные о мощности излучения, длине волны лазера, плотности записи. Схема появления на рынке 2x-дисков выглядела примерно так: сначала изготовитель дисков должен был сертифицировать свое изделие как 1x-совместимое. После этого в сотрудничестве с всемогущей Pioneer болванка доводилась до барьера в 2x. Большая часть доработки заключалась в построении и тестировании отдельной стратегии записи для конкретной серии дисков. Pioneer относительно медленно ведет сертификацию на 2x, объясняя это тщательным отбором претендентов. С «официальными» дисками стандарта 1x-R и 4x-R и 2x-RW дело обстоит намного проще. В перезаписанной области диска, называющейся lead-in, содержатся идентификационные данные диска с разработанной стратегией записи. Для того чтобы начать запись, приводу остается лишь найти в своей прошивке подтверждение на поддержку именно этой серии диска данного производителя. Побочным эффектом от введения стандарта 4x можно считать тот факт, что компаниям-производителям теперь не нужно платить двум «крышам» — DVD Forum и Pioneer. В результате цена на диски для однократной записи 4x не намного больше, чем 2x. А в самом ближайшем будущем можно ожидать, что цена на болванки 4x не только сравняется, но и станет даже меньше, чем на устаревшие 2x.

«Плюс» положительные эмоции

Владельцам рекордеров типа +R/+RW, по-видимому, никогда не узнать, что же порой испытывают хозяева «минусовых» приводов, ведь для них запись на 1x является скорее опцией, которую поддерживают далеко не все программы. Так уж случилось, что «в плюсе» на диски для одноразовой записи существует два стандарта — 2.4x и 4x.

Такие скоростные параметры устраивают большинство пользователей, а это, в свою очередь, не способствует появлению каких бы то ни было «разгонных» модификаций прошивок. И потом, диски типа +R/+RW устроены немного иначе. Эти различия требуют методов, отличных от тех, что применяются для «ускорения» приводов типа -R/-RW. Объясняется это тем, что идентификационные данные пустого диска +R/+RW не записаны в области lead-in, они должны быть извлечены из области, содержащей информацию о физическом формате (Physical Format Information Area) диска в районе адреса 00h. Проблема в том, что такая информация просто не существует на пустом, незаписанном диске. Но в компании Sony, в отличие от Ricoh и NEC, быстрее всего нашли довольно нетривиальное решение этой задачи. Дело в том, что функциональность для относительно старых приводов Ricoh и NEC строилась на использовании мультимедиакоманд третьего, а не четвертого поколения (MMC-3, multimedia commands 3-rd generation). И даже сама возможность запроса адреса 00h не учитывалась. В приводах Ricoh выдается просто сообщение об ошибке. Sony предложила другой подход: привод синтезирует информацию о физическом формате, «вытравливая» нужные данные из ADIP-блока.

Разумеется, с продвижением MMC-4, в котором существует отдельная команда на считывание нужной информации из ADIP-блока, проблема исчезает. Следует лишь дождаться официального релиза с нужной коррекцией. »

▲ Philips стала первой компанией, высказавшейся за стандарт «плюс»

▲ Внешний вид удобной и функциональной утилиты DVDInfo

» Lead-in

Итак, когда возможности по разгону стали представляться более ясно, перейдем непосредственно к делу. Вот тут и возникает главное затруднение. Разбор прошивки каждого отдельного привода в подавляющем большинстве случаев требует индивидуального подхода. Поэтому просто объясним основные положения. Фактически прошивка — это бинарный файл, который был создан при использовании ассемблера. Впрочем, в природе существуют и небинарные прошивки (расширение HEX или MOT). Их придется сконвертировать в бинарный файл, для чего следует воспользоваться соответствующим программным приложением. После этого прошивку нужно будет дизассемблировать. Делать это нужно с учетом специфики используемого в приводе процессора. Пока самыми распространенными считаются Hitachi H8S, Intel 8051, Zilog Z80, Matsushita 102000, Mitsubishi 7902, Hitachi SuperH. Казалось бы, простая операция, но тут на сцене может появиться не видимый до поры до времени результат работы программистов компании, сделавшей привод. Так или иначе, прошивка — разновидность программного продукта, и ее защищают как программу. Pioneer, например, свои прошивки шифрует, Philips и некоторые другие компании предпочитают пользоваться несколько иными методами — в их прошивках используются внешние субпроцессы, которые следят за тем, чтобы доступ к определенным (или всем) полям был закрыт и чтобы статус этих полей не изменялся. Раз по отношению к прошивке этот процесс является внешним, то «обезвредить» его перепрошивкой нельзя. Иногда используются скрытые контрольные суммы, и привод просто не воспримет диск, если проверка этой суммы, включенной в данные диска, не совпадет.

Впрочем, и этот этап можно преодолеть. После прогона в дизассемблере получаем на выходе несколько десятков тысяч строк кода (их может быть 10, 30 или даже 150 тыс.). Теперь в этом коде нужно найти сегмент, в котором хранятся идентификационные данные болванок. Системы как таковой здесь также нет, от версии к версии адреса нужных данных могут кочевать по всему внутреннему адресному пространству прошивки. Такое положение вещей уже само по себе играет роль еще одного защитного барьера. Для того чтобы найти нужный сегмент, имеет смысл искать его по идентификационному коду уже сертифицированной болван- »

Полезная информация

Структура болванки 4x

Любая болванка содержит определенную структуру, достаточно похожую на приведенную нами. Ниже дано описание кода, получаемого в ответ на команду 0E для Read DVD Structure, которая начинается с 4-го байта шестнадцатеричного дампа.

```
00 6A 00 00 01 40 C1 FD 9E D8 52 00 02 35 0E 0B   .j...@....R..5..
FE FF 80 00 03 52 49 54 45 4B 47 00 04 30 34 00   .....RITEKG..04.
00 00 00 00 05 88 80 00 00 00 01 00 06 06 0F 12   ................
A8 88 80 00 07 88 80 00 00 00 00 00 08 05 1B 0E   ................
10 08 09 00 09 97 06 0D 0B 80 00 00 0A 00 00 00   ................
00 00 10 00 0B 06 21 13 A8 87 95 00 0C 99 99 88   ......!.........
80 00 00 00 0D 00 00 D0 00 00 00 00 00 00 00 00   ................
```

1	Код класса принадлежности диска = 40 (диск общего назначения)	**17~30**	Идентификационные данные производителя = "RITEKG04"	**65~70**	2-е поле кода стратегии записи на 4x = 97 06 0D 0B 80 00
2	Физический код диска = C1 (DVD-R)	**33~38**	Код стратегии записи = 80 00 00 00 01	**73~78**	3-е поле кода стратегии записи на 4x = 00 00 00 00 00 10
3-5	Данные о крайних адресах зоны записи = FD9ED8	**41**	Код OPC для 2x (бета) = 06	**81**	Код OPC для 4x при мультиимпульсе (бета) = 06
6	Версия = 52 = DVD-R v2.2 (0x2# — DVD-RW, 0x5# — DVD-R v2, 52 — это DVD-R v2.2.).	**42**	Код OPC для 2x (мощность) =0F	**82**	Код OPC для 4x при мультиимпульсе (мощность) = 21
9	OPC (Optimum Power Calibration) код оптимальной калибровки мощности = 0E	**43~46**	1-е поле кода стратегии записи на 2x = 12 A8 88 80	**83~86**	4-е поле кода стратегии записи на 4x = 13 A8 87 95
10	Код длины волны (для всех дисков однократной записи) = 0B	**49~54**	2-е поле кода стратегии записи на 2x = 88 80 00 00 00 00	**89~94**	5-е поле кода стратегии записи на 4x = 99 99 88 80 00 00
11-14	Код стратегии записи = FE FF 80 00	**57**	Код OPC для 4x (бета) = 05	**97~101**	6-е поле кода стратегии записи на 4 x = 00 00 D0 00 00
		58	Код OPC для 4x (мощность) = 1B		
		59~62	1-е поле кода стратегии записи на 4x = 0E 10 08 09		

Ресурсы в Сети

www.rpc1.org — большой архив разнообразных прошивок для любых приводов. Рекомендуем также посетить форум **http://forum.rpc1.org** — здесь можно почерпнуть много полезной информации.
www.nicsoft.com.au — официальный сайт автора DVDInfo. Новости, результаты тестирования и свежие версии программы.
www.cdrinfo.com — еще один ресурс, посвященный мультимедиаиндустрии. Здесь можно найти любопытную информацию, включая тесты болванок и приводов.
www.cdfreaks.com — прекрасный сайт с весьма богатым содержанием: новости, обзоры, тесты, архив прошивок для приводов и программ для записи и воспроизведения мультимедиаконтента.
www.cdrlabs.com — небольшой, но при этом весьма информативный сайт, содержащий новости и обзоры железа и софта.

» ки. А чтобы узнать его, лучше воспользоваться специальной программной утилитой. Вполне подойдут Nero CD Speed или DVDInfo.

Найти нужные данные в прошивке — это лишь начальная фаза ее изменения. Если нужно в список воспринимаемых приводом болванок добавить новую, то придется не просто найти область, в которой лежат нужные идентификаторы, необходимо обнаружить ее границы и потом уже внести код новой болванки. После этого следует найти соответствующий участок, содержащий стратегии записи, и его начало и конец. Затем создать новую запись с новой стратегией записи. Здесь и лежат основные «грабли», на которые можно наступить. Точные данные о параметрах записи в открытых официальных источниках найти практически невозможно. Остается лишь опыт — свой собственный и чужой. После записи новой стратегии нужно лишь сделать так, чтобы запускаемый приводом процесс по поиску кода и стратегии болванок касался и только что записанных данных. Перед прошивкой привод проверяет то, чем собираются заполнить его память. Проверка касается заголовков и/или контрольных сумм, содержащихся в любой прошивке. Делается это для того, чтобы в память привода не загружали что попало.

Так что придется найти в коде сам алгоритм контрольной суммы, а затем сделать небольшую программку и перекомпилировать созданную вами модифицированную прошивку согласно этому алгоритму. Теперь остается записать прошивку в рекордер и надеяться, что он после этого будет функционировать нормально.

Вот так в общих чертах выглядит модификация пишущего DVD-привода. Достаточно сложный процесс, и не каждый пользователь сможет его провести. Увы, как уже отмечалось ранее, увеличение скоростей чтения или записи является побочным продуктом их деятельности, и такие модификации прошивок в основном созданы для крайне популярных моделей. Найти созданные ими модифицированные прошивки несложно, достаточно посмотреть некоторые из приведенных ссылок.

Да и потом, во-первых, не все компании «приняли меры»: к примеру, NEC пока не была замечена в шифровании и построении серьезной защиты для своих прошивок. Во-вторых, на свете существует достаточно много приводов-клонов (то есть созданных одной компанией по лицензии другой, с сохранением оригинальной конструкторской базы). Благодаря чему в «клон» можно записать прошивку рекордера-оригинала, а это, в свою очередь, позволит получить определенные преимущества: более развитые система поддержки, функциональные возможности, в том числе и в сфере разгона. Не секрет, что OEM-производители иногда «забывают» о некоторых функциональных возможностях привода-оригинала и к тому же реже обновляют прошивки для своих приводов. Все это и множество других факторов говорит о возможности создания «гоночной» версии прошивок для большого числа существующих DVD-рекордеров.

Lead-out

В заключение хотелось бы сказать, что, несмотря на стремительное развитие и совершенствование компьютерной техники, не стоит забывать: «убить» привод при перепрошивке можно так же легко, как, например, и в далеком 1997-м. Поэтому, если вы работаете в основном с брендовыми сертифицированными болванками и вас не огорчают скоростные ограничения, наложенные производителем на привод, вам нет резона лезть в дебри машинного кода и инструкций к флэшерам. Ну а если вы ярый поклонник таких брендов, как Princo и Prodisc, и вас не устраивает списывание родного штампованного DVD-видеодиска на скорости 2x, тогда добро пожаловать в увлекательный мир скоростной записи DVD. ■ ■ ■ **Андрей Шепелев**

Тонкости перепрошивки

Шьем до дыр

Существует несколько разновидностей прошивок для снятия региона. Самая удобная из них сделана по принципу изменения набора инструкций привода. Эти изменения направлены на то, чтобы важный параметр любого видео DVD — CSS Title Key — передавался на хост. Этот параметр нужен для дешифрования содержания диска и его последующего просмотра.
Есть и еще один тип прохождения региональных ограничений — это патч «бесконечной» жизни. В прошивке есть счетчик, содержащий данные об оставшихся попытках изменения зоны. С помощью этой модификации он всегда остается постоянным за счет внесения в него константы. Мы не рекомендуем использовать такой вариант, потому что тип памяти, который используется в прошивках, имеет ограниченное количество циклов перезаписи. Иногда такой ресурс составляет всего 100 циклов. Так или иначе, но подобный патч рано или поздно приведет к сбою NVRAM.
Существует немного иная разновидность «бесконечной жизни». Ее суть заключена в том, что DVD-устройства используют небольшой зарезервированный участок памяти для сохранения результатов изменения региона. Исчерпание лимита памяти приведет к тому, что либо привод попытается переписать соседний участок памяти, в результате чего прошивка будет испорчена, либо привод больше не сможет менять регион. Так что это тоже не самый лучший способ.