

# Транслятор SanDisk

## Общие сведения о трансляторе

В первую очередь, следует отметить, что в современных накопителях Sandisk содержимое микросхемы флэш-памяти может быть зашифровано. К счастью, пока это встречалось только у дорогих накопителей в титановом корпусе, однако, если фирма Sandisk разработала контроллер, поддерживающий шифрацию, то можно предположить, что со временем, шифрация будет внедрена и в другие изделия. Накопители с зашифрованным содержимым в настоящий момент комплексом не поддерживаются.

Далее, следует упомянуть, что у некоторых накопителей Sandisk переставлены байты (а у некоторых – нет). Обычно это выявляется легко. На первой странице обычно содержится слово “Sandisk”. Если оно читается корректно, то байты не переставлены. Если же вместо него написано:

```
0200 61 53 64 6E 73 69 B5 BD F8 4D 18 E6 14 12 FF FF aSdnsicμ½øM.æ..ÿÿ
```

Значит, необходимо установить флажок Byte Swap.

Теперь рассмотрим особенности реализации транслятора. В нём используется не один, а сразу два «хвостика». Первый «хвостик» располагается до данных и имеет длину 6 байт. Второй – после данных. Его длина зависит от конкретной реализации (на настоящий момент известно три варианта длины, но не исключено, что их больше). Первый «хвостик» задаёт данные, относящиеся к транслятору, второй – ECC данных (и интереса не представляет).

Первые 4 байта трансляторного «хвостика» задают номер сектора. На большинстве известных реализаций он в точности определяет номер LBA сектора, но во-первых, известны и иные реализации, во-вторых, может быть несколько секторов с одним и тем же номером.

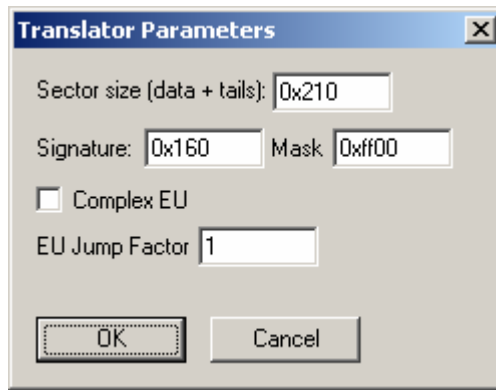
Байты 5 и 6 кодируют состояние сектора. В некоторых реализациях секторы данных кодируются флажками 01 60, в некоторых – 01 00, в некоторых – и теми и другими. Иные флажки обычно не подлежат рассмотрению.

К слову сказать, эти флажки также могут служить быстрым ключом к оценке того, нужна перестановка байтов или нет. Если эти флажки содержат значения 60 01 или 00 01, то следует установить флажок Byte Swap на вкладке Glued Flash.

Кроме того, в современных накопителях блок данных состоит из двух EU, причём эти EU идут не подряд, а отстоят друг от друга на расстояние sizeof(EU)\*3. Предположительно, это ускоряет работу с многоплановыми микросхемами.

## Работа с образами Sandisk

После первичного анализа образа, программа выдаёт следующий диалог «тонкой» настройки:



Поле Sector Area (data + tails) задаёт размер одного сектора. Этот размер рассчитывается автоматически. Как уже отмечалось выше, данный параметр может быть равен 0x210, 0x214, 0x216. Возможно – бывают и другие значения. Если параметр не менее 0x210 и не более 0x230, то скорее всего, он рассчитан корректно.

Поля Signature и Mask задают сигнатуру «хвостика», которую следует считать сигнатурой сектора данных. Как уже упоминалось ранее, сигнатура может быть 01 60, 01 00 и смешанная.

Сигнатура	Поле Signature	Поле Mask
01 60	0x0160	0xffff
01 00	0x0100	0xffff
Смешанная	0x0160	0xff00

В целом, рекомендуется задавать значение для смешанной сигнатуры, а если транслятор не собирается – использовать более тонкую настройку.

Флажок Complex EU будет взведён, если обнаружится, что блок располагается в двух EU сразу. А значение EU Jump Factor задаёт расстояние, на которое вторая половина блока отстоит от первой (обычно это значение равно трём).