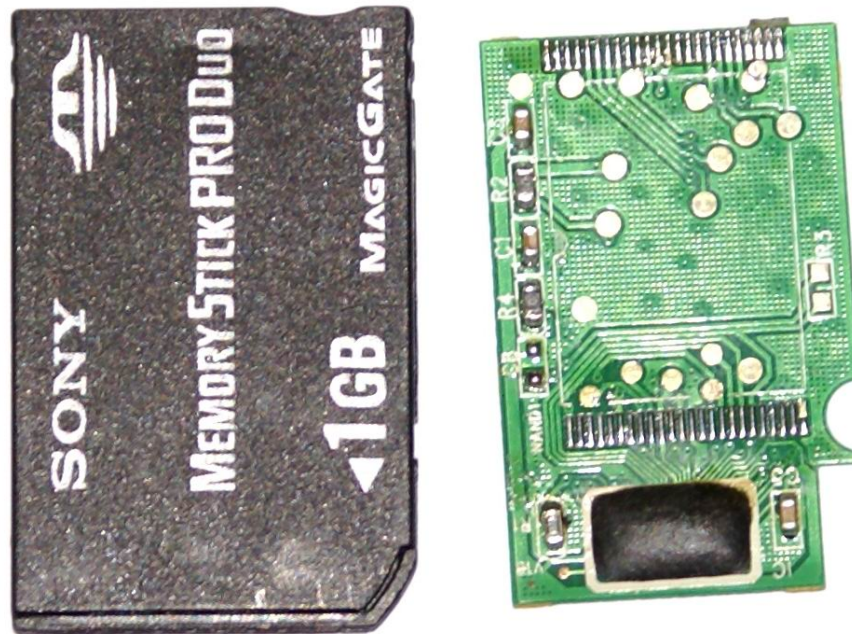


Транслятор псевдо SONY Memory Stick

Формально, данный транслятор применён в накопителе Sony Memory Stick PRO Duo, однако, есть все основания считать, что накопитель является подделкой под известную марку. В содержимом флэш-памяти, не найдено ни одной строки со ссылкой на SONY, на микроконтроллере отсутствует маркировка (он вообще выполнен в бескорпусном исполнении).



Как всегда, находим сектор, заполненный нулями, чтобы выявить формат «хвостиков». Выясняем, что формат – стандартный «SBD». Теперь переключаемся в режим отображения «хвостиков» для SBD формата.

EU=0x8C	Pg=0x2300	D7 59 D9 3C 06 48 0F 0F	3E 3E	57 00	AA FF FF FF
EU=0x8D	Pg=0x2340	E6 CD 15 F4 D5 72 0A 0A	3E 3E	57 00	AA FF FF FF
EU=0x8E	Pg=0x2380	47 77 EA 2D 08 08 07 07	3E 3E	4B 00	CC FF 00 00
EU=0x8F	Pg=0x23C0	76 E3 26 E5 DB 32 02 02	3E 3E	4B 00	CC FF 00 00
EU=0x90	Pg=0x2400	50 29 56 3D 26 E7 03 03	3E 3E	14 00	AA FF FF FF
EU=0x91	Pg=0x2440	61 BD 9A F5 F5 DD 06 06	3E 3E	14 00	AA FF FF FF
EU=0x92	Pg=0x2480	F7 1D DC 0A 58 25 06 06	3E 3E	9B 00	AA FF FF FF
EU=0x93	Pg=0x24C0	C6 89 10 C2 8B 1F 03 03	3E 3E	9B 00	AA FF FF FF
EU=0x94	Pg=0x2500	62 65 D5 32 7E 5F 0B 0B	3E 3E	4E 00	CC FF 00 00
EU=0x95	Pg=0x2540	53 F1 19 FA AD 65 0E 0E	3E 3E	4E 00	CC FF 00 00
EU=0x96	Pg=0x2580	ED 44 DB BE 09 AB 05 05	3E 3E	3E 00	AA FF FF FF
EU=0x97	Pg=0x25C0	DC D0 17 76 DA 91 00 00	3E 3E	3E 00	AA FF FF FF
EU=0x98	Pg=0x2600	67 33 EF 1B 56 65 0E 0E	3E 3E	87 00	AA FF FF FF
EU=0x99	Pg=0x2640	56 A7 23 D3 85 5F 0B 0B	3E 3E	87 00	AA FF FF FF
EU=0x9A	Pg=0x2680	E3 BC A6 A9 0B 18 05 05	3E 3E	4C 00	AA FF FF FF
EU=0x9B	Pg=0x26C0	D2 28 6A 61 D8 22 00 00	3E 3E	4C 00	AA FF FF FF
EU=0x9C	Pg=0x2700	F2 4B E6 23 70 1F 03 03	3E 3E	52 00	CC FF 00 00
EU=0x9D	Pg=0x2740	C3 DF 2A EB A3 25 06 06	3E 3E	52 00	CC FF 00 00

Бросается в глаза сигнатура 3E 3E. После неё идёт номер блока в формате IntelFFF.

Однако, если собрать накопитель, воспользовавшись стандартными методами, то он соберётся некорректно. Да, у накопителя будет найдено строго 8 банков. Но всё равно что-то не так. Если банков строго восемь, то конфликтов быть не должно, а они – есть. Следовательно, что-то не так с размером банка. Если собрать статистику, где встречаются одинаковые номера блоков, то выясняется, что размер банка не равен 1/8 от размера флэш-памяти. Мало того, некоторые сектора, которые относятся к FAT, размещены где-то в конце адресного пространства. При этом, у транслятора явно отсутствует чередование адресов и прочие неприятности, которые мешают жить ремонтнику.

Анализ показал, что при количестве страниц 0x80000, только 0x7B000 страниц отведено под банки. И именно пространство от 0 до 0x7AFFF разбито на восемь равных частей. Начиная же с 0x7B000, идёт пространство, в котором могут быть данные из любых банков. В самом худшем случае, там могут встретиться блоки из всех восьми банков. При этом, внутри самих банков блоки с соответствующими номерами будут отсутствовать.

Чтобы учесть эти особенности транслятора, в INI файл следует добавить следующий ключ:

Extra Bank Size=0x28

Откуда взёлось «волшебное» число 0x28? Всё очень просто.

Исходим из того, что у микросхемы один EU равен 0x40 страниц.

Гигабайтная микросхема содержит 0x80000 страниц. $0x80000/0x40 = 0x2000$ EU.

Как выяснилось экспериментально, реально под блоки отдано 0x7B000 страниц (вычисления велись интуитивно), или $0x7B000/0x40 = 0x1EC0$ EU.

Рассчитаем разницу. $0x2000-0x1EC0=0x140$. Столько EU выделено под дополнительный банк.

Чтобы не быть привязанными к объёму накопителя, рассчитаем, по сколько EU «отщипнули» от каждого банка: $0x140/8=0x28$. Вот это и есть наша «волшебная» константа.

Для закрепления материала, рассмотрим чисто теоретический пример, что было бы, если бы размер EU был не 0x40, а 0x100 (у микросхем большой ёмкости такое возможно, так что пример в будущем может пригодиться).

Полная ёмкость $0x80000/0x100=0x800$ EU

Урезанная ёмкость $0x7B000/0x100=0x7B0$ EU

Разность $0x800-0x7B0=0x50$

На один банк приходится $0x50=0x0A$ EU

То есть, «волшебная константа» будет равна 0x0A.