алхимия прошивки видео-BIOS

крис касперски ака мыщъх, no e-mail

экстремальный разгон требует экстремальных мер — наращивания тактовой частоты, увеличения напряжения, смены прошивки. нам нужен точный рецепт, чтобы соединить все эти реагенты воедино и получить желаемый результат. и этот рецепт лежит перед вами ### находится в ваших руках!

введение

Разгон видео-карт — это настоящий дзен! Покруче буддизма будет! Как говориться, видео-карты доступы всем, а достигнуть нирваны удается не каждому. Существует множество хороших утилит типа **RivaTuner,** волей Аллаха творящих настоящие чудеса, но всех их настройки заключены в руках Будды, священные свитки машинного кода которого хранятся в недрах BIOS, в лабиринтах которого ориентируется только посвященный.

Еще никто не проходил этот лабиринт до конца, но кое-какие тоннели уже исследованы и даже картографированы. В них хранится столько сокровищ и артефактов, что буквально рябит в глазах. То полигоны слетают, то появляются какие-то стремные точки в самых неожиданных местах. Спокойно, парни! Это не глюк! Нормальный глюки уже давно обломались. Это просто кривой разгон такой. Совсем не даосский разгон скажу я вам. Сейчас мыщъх покажет, на что способен BIOS и как разогнать систему так, чтобы она не изменяла и не высаживала.

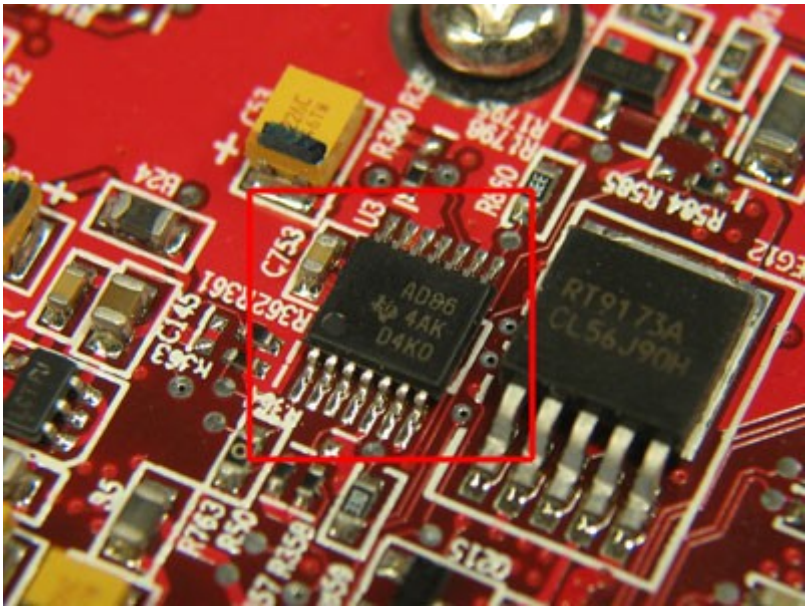

Рисунок 1 BIOS – это такая небольшой "таракан" на плате, иногда установленный в панельку, иногда намертво припаянный к ней

цели и возможности перешива

Прошивка — это еще не вся видео-карта, а только ее часть. Вроде бы простая истина, но не все врубаются в нее с первого раза. Выше железа все равно не прыгнешь, ведь за его пределами ничего нет. Только сплошное зависалово и глюкодром. Штатный BIOS реализует определенный потенциал, определить который заранее невозможно. Китайцы выжимают из железа все, что можно и дополнительный разгон валит карту как под Полтавой. Серьезные производители оставляют солидный запас прочности, который не грех поиметь и напрячь.

Подлая натура восточно-американского менталитета ограничивает предельные значения тактовых частот и таймингов, которые только можно установить программным путем (со штатной панели управления или твикером). И это еще не все! Блокируются целые модули, опции и режимы передачи данных (дополнительные пиксельные конвейеры, адресация по побочной шине и др. возможности), физически реализованные в железе, но недоступные

программно! А как насчет тех пакетов и утилит, что проверяют идентификатор производителя, отказываясь работать с "неродной" картой, несмотря на то, что она полностью совместима со своим оригиналом?

Вы уже материтесь? Ну и зря. Умные люди это только приветствуют. Чем больше на карте заблокированных возможностей, тем эффективнее разгон. Мы не только экономим деньги, "превращая" дешевую модель в более дорогостоящую (в частности, GeForce 6800 физически имеется 6 пиксельных конвейеров, из которых штатно доступно только 5), но и получаем глубокое моральное удовлетворение, от того что на$%^@# (перехитрили) производителя, а это — важнее всего!

Вот тут некоторые интересуются — насколько законен разгон? Формально, с точки зрения законодательства, с видео-картой, приобретенной законным путем, мы можем делать все, что угодно и никто не в праве нам помешать. Производителям, естественно это ни хрена ### совсем не нравится и они апеллируют к авторскому правому. Как будто бы прошивка есть его объект. Как будто бы авторское право запрещает модификацию. Все это гон! Читать уголовный кодекс от забора и до обеда! Идем в магазин, покупаем книжку, делаем в ней кучу пометок, в стиле "дорвалось дите до карандаша", ну и что? Топать сдаваться в прокуратуру, ведь "модификация" на лицо? Да никакой закон не запрещает модифицировать что бы то ни было, но, внимание на монитор (!), дает продавцу (и производителю) права забрать все свои обязательства назад и послать нас куда-то очень далеко. Модификация BIOS'a — очень деликатное дело (это вам не траву драть!) и если сделать что ни будь не так, видео-карте может сильно поплохеть, вплоть до выхода из строя, но тут каждый решает сам — рисковать или нет. Кстати говоря, у карты на кремнии не написано, что она сдохла из-за наших экспериментов с BIOS'ом. Идем в гарантийный отдел, прикидываемся байтом и пускай попробуют что-то доказать. Только на психику лучше не давить. Если там здорово разозлятся, докажут так, что не соберешь, но только навряд ли.

Так что откинем левые мысли прочь и начнем. А начнем мы с разблокирования заблокированных фич.

Рисунок 2 при чрезмерном разгоне карты возможно появление артефактов (artifacts) – разнообразных искажений и дефектов изображения типа "вылета" полигонов, разноцветных точек в разных местах, полос на сплошных фонах, самопроизвольно меняющихся цветов графических элементов и т.д.

Рисунок 3 вылет двух полигонов

>>> врезка плюсы и минусы SBA

SBA (Side-Band Addressing адресация по побочной шине) это такой режим передачи данных, при котором адрес запрашиваемого блока передается по дополнительной 8-битной шине, в то время как предыдущий блок передается по основной 16-битной шине, что значительно увеличивает производительность (по тестам).

А вот в реальной жизни выгода от SBA не столь очевидна. Прирост производительности в играх практически незаметен, к тому же дополнительные 8-бит ухудшают помехоустойчивость AGP-шины, затрудняя ее разгон, не говоря уже о том, что многие материнские платы и AGP-драйвера настолько криво поддерживают SBA, что использовать его все равно не получается. Тогда какой смысл его разблокировать?

в погоне за разгоном или что можно гнать

Разгон BIOS'a держится на трех китах: тактовой частоте, таймингах и напруге. Это довольно вздорная семейка, которую непросто примирить. Неправильное сочетание параметров ведет к перекосам, глюкам и тормозам. Из карты уже дым идет, а производительность падает ниже штатной. Вот такое непростое дело разгон. Легкая жизнь бывает только в раю. Соблюдай заповеди, слушайся производителей и да проведет тебя инструкция прямым неизогнутым путем к… таким же лахунднрам как и ты. Буддизм рая не обещает. Достигнуть нирваны может только тот, кто отречется от мира и конкретно зависнет в компьютерном храме, обложив себя технической документацией. Включит паяльник и раскурит кальян, набитый канифолью и принтерными распечатками, которые, кстати говоря, очень недурно дымят.

Короче, значит, ***частота***. В смысле меандр. Это сигнал такой. Тактирующий. А тактировать он должен графический процессор и память, а так же все блоки их сопрягающие. Меандр вырабатывается осциллятором (он же кварц), обычно генерирующим 14.318 MHz (старые видео-карты) или 27 MHz (новые). Это — базовая тактовая частота, еще называемая эталонной или опорной. Все остальные частоты формируются путем умножения базой часты на множитель x, изменяемый с шагом от 0,25 до 1. Конкретное значение зависит от конструктивных особенностей отдельно взятой модели и чем оно меньше, тем лучше.

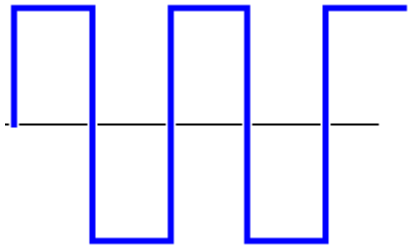

Рисунок 4 сигнал типа меандр

С увеличением тактовой частоты возрастает нагрев, следовательно, необходимо позаботиться о хорошем охлаждении. Предельное значение множителя упирается в напряжение, которое необходимо увеличивать вместе с таковой частотой. Чем выше напряжение, тем быстрее происходят переходные процессы в кристалле, однако, вместе с тем выше и нагрев, который растет как сумасшедший, ускоряя дегенеративные процессы в миллионы (!) раз, а это значит, что кристалл может отказать в работе через несколько лет, месяцев или даже дней. Появится глюки, избавиться от которых снижением напряжения/частоты уже не удастся! Так что тут главное не перегнать!

Разгонный потенциал графического процессора и памяти неодинаков, на некоторых картах лучше гонится процессор, на некоторых — память (ну вообще-то память при наличии паяльной станции или даже простого паяльника с бритвенным лезвием можно и перепаять, но это уже будет экстрим). Наивысшая производительность достигается лишь при определенных соотношениях частоты процессора и памяти. Обычно — это кратная частота, то есть частоты памяти/процессора соотносятся как целые числа, например 1:2, но тут бывают и исключения. Как правило, производитель уже нашел "золотую середину", от которой мы можем "плясать", увеличивая обе частоты на один и тот же множитель одновременно (именно множитель, а не абсолютное значение частоты! — учите мат. часть!)

В серии GeForce 7800 (и некоторых других моделях видео-карт) графический процессор тактируется не одной тактовой частой, а сразу тремя! Различные блоки могут работать на различных частотах, значительно повышая свой разгонных потенциал. Обидно, что разработчики фирменных драйверов до сих пор не используют эти возможности, изменяя частоту блока растеризации (ROP) и блока пиксельных шейдеров (Shader Unit) синхронно с частотой блока геометрии, в то время как "железо" позволяет настраивать всю эту троицу строго индивидуально. Единственная оставленная нам лазейка — параметр geometric delta, определяющий превышение частоты блока геометрии по отношению к остальным блокам. Только воспользоваться ей на практике все равно не удается. Шаг изменения тактовой частоты блока геометрии меньше шага остальных блоков, поэтому их частоты меняются скачкообразно, что для разгона очень нехорошо. Даже хреново. Но это не ограничение железа, а только голимых драйверов. Модификация BIOS'а позволяет решить проблему.

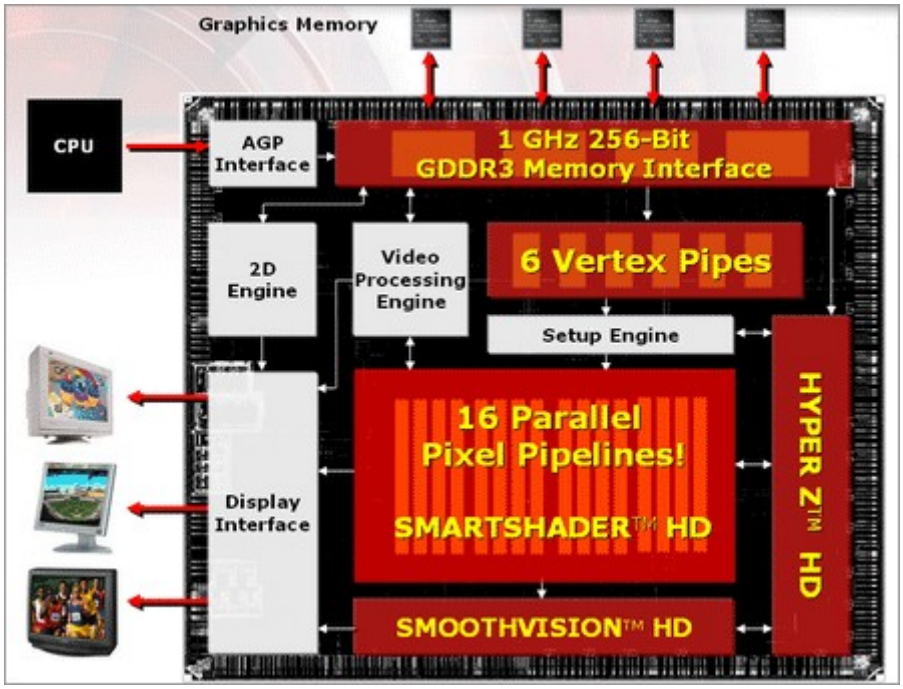

Рисунок 5 графический процессор состоит из множества блоков и на современных картах эти блоки могут работать на "своих" тактовых частотах

Впрочем, меандр по любому это отстой и ерунда. Опытные конструкторы еще со времен Z80 знают, что логику лучше всего тактировать короткими импульсами, "отстающими" или "опережающими" процессор в зависимости от машинных циклов, правда, сказать это __намного__ проще, чем спаять. Вот и паяльник вам в руки! (главное, чтобы не в задницу).

Рисунок 6 графический процессор — самая главная микросхема на плате, лежит себе и не знает как круто мы ее будет разгонять

вольтаж и вольтмод

Управлять напряжением намного сложнее, чем накручивать тактовую частоту. Не у всех это получается или получается, но не совсем. Разнообразные утилиты утверждают, что напряжение изменилось, но проверка вольтметром не обнаруживает никакого приращения. Из этих двоих кто-то нагло врет. И это явно не вольтметр.

hex-редакторы показывают, что внутри BIOS'a существует специальная таблица: одна колонка — напряжение в вольтах умноженное на 100, другая — соответствующий этому напряжению идентификатор (VID). Другая таблица сопоставляет идентификаторы с режимами производительности. Таким образом, "табличные вольты" внутри карты никак не используются и нужны только утилитам мониторинга. Патичить их можно, но бесполезно (то есть, почему бесполезно, пропатчить их до 1000 вольт и потом хвастаться друзьям, что у нас стоит карта военного образца на атомном дизель-генераторе). Реальное напряжение определяется идентификатором. Каждому VID соответствует своя комбинация логических нуля и единицы, подаваемых на вход стабилизатора и вот эта комбинация и рулит. Изменить ее можно только путем редактирования BIOS'a, а точнее той его части, что взаимодействует со стабилизатором.

На карте существует четыре основных потребителя электричества, каждый из которых питается своим напряжением, это:

- Vgpu - напряжение питания ядра;
- Vdd - напряжение на входных буферах, ядре памяти;
- Vddq - напряжение на выходных буферах памяти;
- Vref - эталонное напряжение для входных буферов;

Где-то в недрах BIOS'a должно быть четыре таблицы VID → комбинация, однако, не каждая карта позволяет менять все четыре напряжения программно, да нам это и не нужно. Обычно, при разгоне увеличивают только напряжение питания графического ядра. Напряжение на памяти лучше не трогать, особенно если она без радиатора, а радиатор клеиться двухсторонним скотчем, который можно найти в строительных магазинах или термоклеем. Короче, намек понят.

Если программными средствами изменить напряжение не удается и стабилизатор полностью реализован в "железе", приходится идти другом путем. Находим на плате резистор, ответственный за выбор напряжения на стабилизаторе (загляните в схему микросхемы стабилизатора, которую можно найти в интернете по его марке), и проводим несколько линий на его корпусе обычным мягким карандашом так, чтобы они соединяли оба вывода. Варьируя количество и толщину черточек, мы можем изменять напряжение в некоторых пределах. Не очень надежно, но все-таки. А еще можно приклеить дополнительный резистор или даже повесить его на проволочную петлю. Однако, это уже экстрим. Причем суровый. Для тех, кто хочет им заняться — ищите в Гугле по ключевым словам "вольмод" (voltmod).

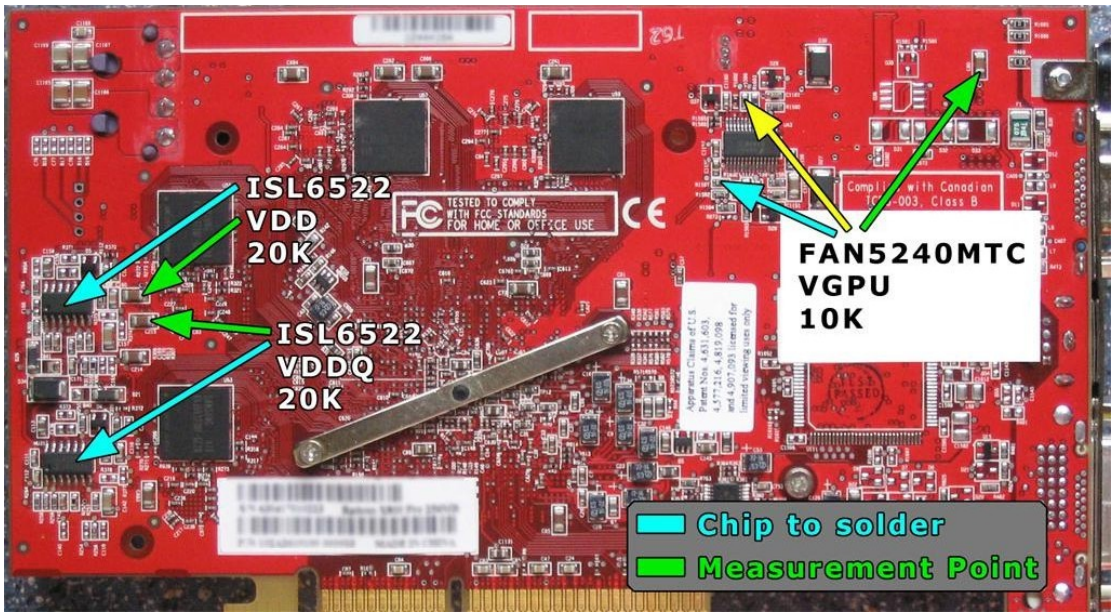

Рисунок 7 резисторы, ответственные за разгон карты nVIDIA GeForce4 MX

где брать прошивку

Прошить BIOS немудрено, это сумеет даже ламер. Сложнее найти… Нам ведь нужна не любая прошивка, а "правильная", то есть разогнанная. Начнем с фирменных сайтов. Сайтов конкурентов. В борьбе за клиента они частенько хачят оригинальные прошивки, выжимая из железа все, что возможно. Например, можно засунуть внутрь nVIDIA GeForce FX5900 прошивку от ASUS 5900SE, в которой отсутствует разделение частот в 2D/3D и сильно досаждающий всем overclock'ерам "автотормоз".

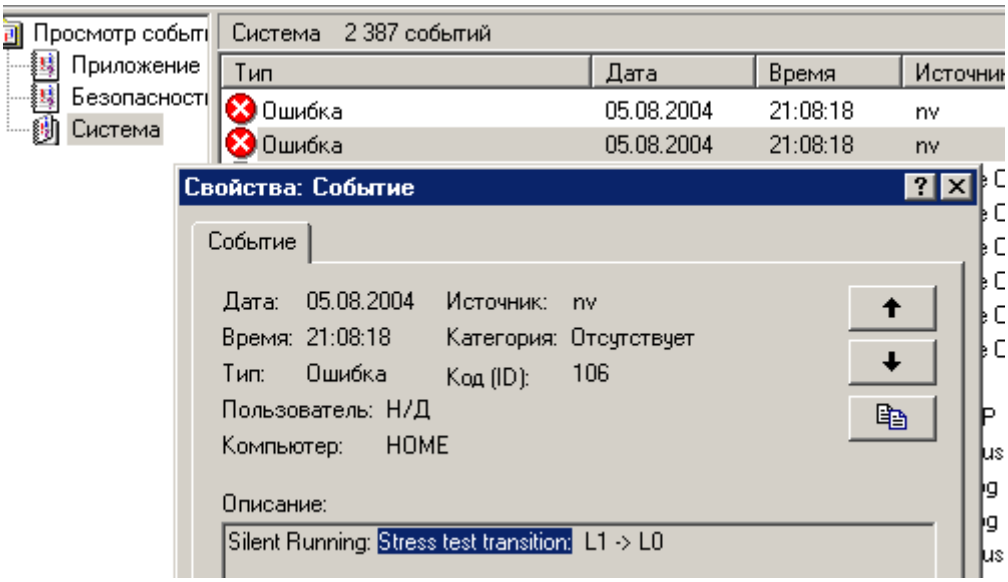

Рисунок 8 многие карты имеют защиту от разгона, автоматически сбрасывающую тактовую частоту при перегреве и заносящую соответствующую запись в системный журнал Windows.

Неплохой результат дает использование прошивки от более "крутой" модели того же самого производителя, например, ATI Radeon 9800Pro →ATI Radeon 9800XT или nVIDIA 5900 →5950Ultra (естественно, карты должны быть совместимы между собой на "железном" уровне).

Многие драйвера, прошивки и некоторый "фирменный" софт проверяют версию карты перед установкой, чтобы быть уверенными, что им не подсунут "чужое" железо. Существует три уровня проверок:

- SubVendor/SubSystem ID (идентификатор вендора), прошитый внутри BIOS и легко исправляемый hex-редактором или твикером типа RivaTuner;
- PCI DeviceID (идентификатор PCI устройства), в зависимости от конструктивных особенностей карты задаваемый либо комбинацией резисторов на видео-карте, либо защитный в BIOS. его так же легко изменить, даже не прикасаясь к паяльнику. резисторы не висят на шине. их считывает BIOS и правильным образом хакнтуая прошивка может прикинуться чем угодно: хоть кроликом, хоть слоном (да слон, я слон, только ногами не бейте);
- GPU Version — (версия видео процессора) определяется внутренними регистрами видеопроцессора, изменить которые невозможно в принципе, однако, чтением их содержимого опять-таки занимается BIOS, которую можно заставить рапортовать все, что угодно.

По умолчанию, утилиты прошивки отказываться перешивать BIOS, если идентификатор вендора/PCI устройства не соответствует действительности, однако, это ограничение легко обойти, форсировав принудительную прошивку специальным ключом командной строки, описание которого можно найти в сопроводительной документации или встроенном help'e. В частности, утилита nvflash от nVIDIA вызывается так: "nvflash -4 -5 -6 имя_файла", правда если прошивка пройдет неудачно, никто отвечать не собирается.

Только все равно, радикально разогнать карту таким образом не получится. Много хороших прошивок встречается на различных хакерских форумах и железячных сайтах. При некотором усердии прошивку можно хакнуть и самому, но для этого необходимо уметь дизассемблировать и уверенно держать ИДУ в руках. Впрочем, есть один хитрый трюк, который легко освоить. Большинство значений (например, тактовых частот) лежат в прошивке "прямым текстом" и могут быть найдены элементарным контекстным поиском в HIEW'e или любом другом hex-редакторе. Допустим, нам известно, что карта поддерживает следующий ряд тактовых частот: 300 MHz, 350MHz, 375MHz и следующий ряд напряжений 0,64 В и 1,56 В. Как их найти в прошивке? Очень просто! Умножаем все числа на сто, переводим в hex-систему (это можно сделать, например, с помощью стандартного Windows-калькулятора, в "инженерном" режиме или самом HIEW'e, нажав <Alt>+<=>, затем только остается поменять местами старший и младший байты, поскольку в x86 процессорах младший байт традиционно располагается по меньшему адресу, а в "арабской" нотации наоборот.

Вот что у нас получится: 300 → 30000 → 7530h → 30h 75h; 350 → 35000 → 88B8h → B8h 88h; 375 → 37500 → 927Ch → 7Ch 92h; 0,64 → 64 → 40; 1,56 → 156 → 9Ch. Следовательно, нам необходимо найти числа: 30h 75h; B8h 88h; 7Ch 92h; 40h и 9Ch. Вскрываем прошивку в HIEW'e и… все это там действительно есть! Главное — не попасться на удочку ложных срабатываний, т. к. эти же числа могут встречаться совсем в посторонних местах. Как отличить какие из них наши? Ответ — "правильные" числа будет сгруппированы в одном районе. Вот они (см. рис. 9)

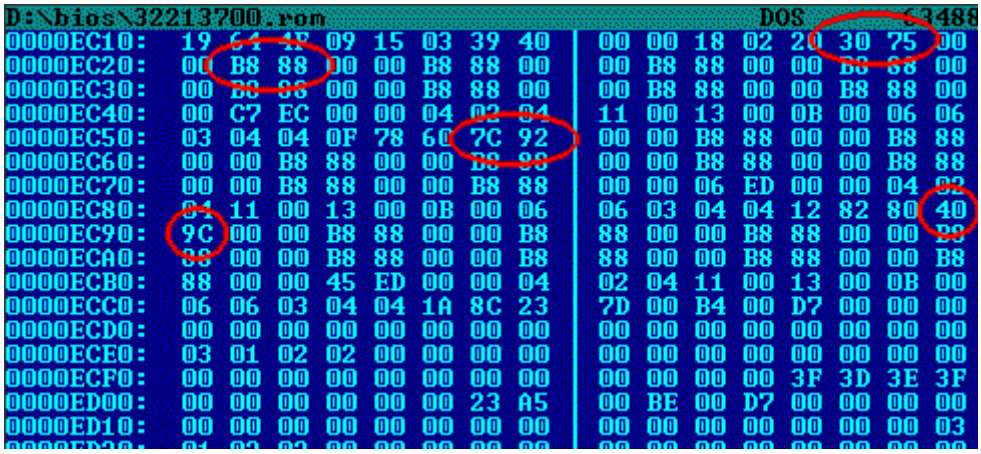

Рисунок 9 хачинье прошивки в HIEW'e

Теперь мы можем исправить их на любые другие значения, которые нужны нам (напоминаем, что захачить таким образом напряжение не получится), после чего обновленную прошивку можно заливать в BIOS, но предварительно необходимо пересчитать ее контрольную сумму, иначе карта откажется подключать ее. Это можно сделать с помощью все той же утилиты прошивки.

если прошивка прошла неудачно (вместо заключения)

Каждый хакер должен быть готов к тому, что прошивка пройдет неудачно и карта покажет черный экран. Что тогда? Многие faq рекомендуют воткнуть ISA или PCI карту, указать в BIOS Setup, что она теперь главная, и грузиться с нее, перешив BIOS еще раз. Однако, найти материнскую плату с ISA слотом можно только в музее, да и PCI шина начинает сдавать.

Правильные мыщъх'и создают загрузочную дискету (а создать ее можно, например, из Windows 9x), прописывают в autoexec.bat все необходимые строки, так чтобы утилита прошивки запускалась автоматически без участия человека и… все. Если нет дисковода, можно создать загрузочный CD. Главное — чтобы файл прошивки был размещен на самой диске/CD, а не на жестком диске, т.к. NTFS-разделы из MS-DOS ни хрена не видны. Только убедитесь, что дискета действительно читается, и все настроено правильно!

>>> ссылки на утилиты для прошивки

- **NVIDIA BIOS Editor**:

- отличный редактор BIOS'а видео-карт от nVIDIA, может редактировать образ прямо в тенях, поддерживает множество опций и распространяется бесплатно: http://www.nvworld.ru/downloads/rvbsetup.exe;

- **NiBiTor**:
  - правит BIOS в файле образе, поддерживает множество опций, бесплатен: http://www.mvktech.net/component/option,com_remository/Itemid,26/func,selectfolder/cat,92/page,2/;
- **VGA BIOS**:
  - позволяет загружать BIOS в оперативную память и работать с ним из MS-DOS, что очень полезно для проверки работоспособности хакнутых прошивок: http://www.nvworld.ru/downloads/VGABios.zip;
- **RivaTuner:**
  - замечательный твикер, поддерживающий огромное количество различных настроек и позволяющий делать с картами nVIDA и частично ATI что угодно: http://www.guru3d.com/rivatuner/;

Рисунок 10 логотип программы RivaTuner