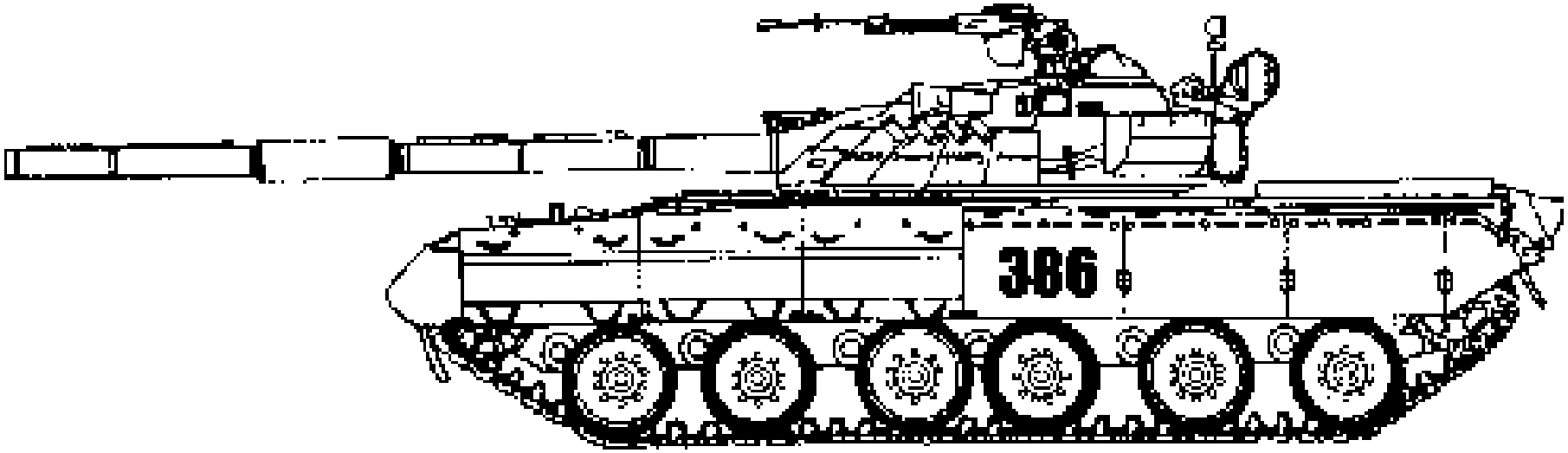


80_PA

альтернативная (хакерская) реализация технологии онлайн-активации SecuROM PA (Sony DADC AG)

«Тибериумный реверсинг»

2011-2026

«Когда пиратство берет верх над DRM, а пираты оказываются гораздо сильнее людей, которые с ними борются. Йохохо!»

ОГЛАВЛЕНИЕ

1. 80_PA. Важная информация. Ответы на вопросы ____ 4
2. 80_PA. Краткое описание технологии онлайн-активации SecuROM. Терминология ____ 8
3. 80_PA. Процедура генерации правильного unlock code. Описание возможных ошибок и их устранение ____ 12
4. 80_PA. Проводник по окнам ____ 29
5. 80_PA. Android com.lab_80pa ____ 38
6. 80_PA. Раскрытие исходного кода генерации HWID и структур unlock (request)code ____ 39
7. 80_PA. Другие проекты ____ 47
8. 80_PA. О проекте 80_PA. Обратная связь ____ 50

оригинальные хэши

V 1.1:	***MD5:*** 8a4d3601e76c6fbfabed3f72695fd042	***SHA1:*** ae30188a993d26b3e442aee58df6db02b5934fa2
V 1.2:	***MD5:*** e30aa4d4615b2c237a63d06039f7fb12	***SHA1:*** 787c8f7a90c23d77a0ade0e781926dee730c9539
V 1.2.1:	***MD5:*** 7371519521cd3f18a097c9160aed48b1	***SHA1:*** d9dcf7add7b69c0fdc5af0473a52bfe8a58071c1
V 1.2.1 hotfix:	***MD5:*** b67a7d6050f5ecc727c89d925a2d6b69	***SHA1:*** ddafd26396b18cfd66a96e2273f0803bb326766d
V 1.2.2 hotfix:	***MD5:*** c06535fee8af5620f7023e2ff91c7f79	***SHA1:*** 7a8b8d1c92477fd789acce34bc9253c659c3678c
V 1.2.3 hotfix («Chinese edition»):	***MD5:*** 3622da94e73da6f74ccc1c02e80b6aa4	***SHA1:*** 8cb081cdeac02a03697ba52df0fa1a4bca451b93
V 1.3.0 big update:	***MD5:*** ff33b0d5ae28f0f90e75300929d1ce68	***SHA1:*** b61f483d12c856f3916091cbeca273b0f27d219d
V 1.3.1 hotfix («Telltale edition»):	***MD5:*** db2cc965529de727e544291a0aa69004	***SHA1:*** 2b3f08c52b4033caf4c7e96db6179ba55466416a
V 1.3.2 hotfix («over 100 key kits...»):	***MD5:*** b4646055708121874247 8f8d5585e995	***SHA1:*** 90ca6fe4620a6b03f2a9dc56d02a0c93eeb505a7
V 1.3.3 hotfix («"review update...»):	***MD5:*** 91510d698fb57b870acef168d668119d	***SHA1:*** fe139441f8bece2731439462dfc9c957da9a7031
V 1.3.4 hotfix («"kav update...»):	***MD5:*** 43a34a79764c2fe0069fb23041ce0781	***SHA1:*** 43d3f187006a7a49adfa05876be7cea886b072e5
V 1.3.5 hotfix («"five»):	***MD5:*** 90aa774709a255f47ea1ea908b521f1c	***SHA1:*** 5759cc7a3db467157b2e33cf07f805555a75a364
V 2.0 («2020»):	***MD5:*** 78259f563deb8b857cd63c1d4e08c010	***SHA1:*** 3bbde1fbe3865cf2e89ee83a56932e3c46485271
V 2.0 hotfix («2020»):	***MD5:*** 71040679a0a0a85ca12f4bfb0edbb3fe	***SHA1:*** fe4125af9e378caea4b8f4bf921a6be6d12bbebd
V 2.0 new («2022»):	***MD5:*** D7E142142D470E5FC9642BC3253FD612	***SHA1:*** 72326EF9AC18B60F2B3BD32A37D2679A58AC56EC
V 2.0.3 («2023»):	***MD5:*** 4B44BA20D5DA3814E47A96CA7CFC7B2C	***SHA1:*** 766331908D00D3B10A42E9BEB2AA173BFA67DF3B
V 2.1.0 («2023_761»):	***MD5:*** 98AAE36593F3D578C81985099C4ACB4F	***SHA1:*** 070C2AE1235A6075B4A2D8801E7ED14DCB363858
V 2.7.0 («07/2023»):	***MD5:*** D21356EFCDD798B76B1EAD4CBD0A87DD	***SHA1:*** ED6D8E36E1709596E4E70B12260FE3B3D5733727
V 2.7.1 («10/2023» - 600):	***MD5:*** 742B60209D6FC8CA530A586507DC6B25	***SHA1:*** 73CDE0FADCC28DE692C58FA02D1653271CB8E39D
V 2.7.2 («04/2024» - rampage!!!):	***MD5:*** 7662FED60C37541A8D0EE7EF31B7D9AF	***SHA1:*** 79584814FC935E7071C5CDB70DCC62FF8651DA4C
V 2.7.3 («07/2024» - rampage2!!!):	***MD5:*** 300EA5353106F1CF868DFA55808EC8DD	***SHA1:*** 32FBC21AAF02575A005411EDDE234607C25DCE4D
V 2.7.5 («03/2025» -yates edition):	***MD5:*** 07864AC225831229C904C4B020043B37	***SHA1:*** 8A50634BE26A19DD0026873A0992472D9BF005A0
V 2.7.7 («01/2026» -CRISTRMAS):	***MD5:*** FA0DECA6D382EC78D7FAEBF9BC80C325	***SHA1:*** 75408381FF298CE7C0DA57961C4A2915E2723B01

Важная информация. Ответы на вопросы.

Зачем нужен 80_PA? В первую очередь, чтобы поиздеваться над Sony DADC AG и лично Рейнгардом Блауковичем. А по существу: если Вы пользуйтесь лицензионными копиями игрушек с SecuROM PA, то можете, совершенно легально, используя *80_PA*, регистрировать эти самые игрушки в обход официального без знания серийного номера (s/n). Причем сюда же попадают игрушки с режимом SecuROM «Trial mode» (например, от компании *«Big Fish Games»*) и *EA Game Authorization Management*, где, с помощью нехитрых ухищрений, заставить SecuROM активироваться вручную (Manual activation).

Касаемо распространения исполняемого файла и предоставления исходных кодов. Исходный файл *80_PA.exe* можно и нужно распространять на любых интернет-ресурсах, не забывая также прилаживать данную инструкцию по использованию. Приветствуется указание ссылки на первоисточник https://exelab.ru/f/PAUnlock. Оригинальный исходный код 80_PA (кроме функции генерации SecuROM HWID и некоторых вспомогательных) пока не распространяется публично и имеется в наличии у некоторого круга заинтересованных лиц. Продажа и перебивка копирайтов не допускаются. Если у Вас есть желание разобраться с технологией онлайн-активации SecuROM – НАПИШИТЕ АВТОРУ ПРОГРАММЫ!

Касаемо вредоносного содержания исполняемого файла. Скачивайте «80_PA.exe» только из доверенных источников (exelab.ru, cracklab.ru, antistarforce.com, rutracker.org, ~~securom.com~~, ~~denuvo.com~~)! Исходный оригинальный файл *80_PA.exe* НЕ содержит никакого деструктивного и вредоносного кода и НЕ может принести вред Вашему компьютеру. Подавляющее большинство кода представляет из себя криптографические операции, взятые из проектов OpenSSL (https://www.openssl.org/source/) и BigDigits (http://www.di-mgt.com.au/bigdigits.html). Остальная информация была получена путем реверс-инжиниринга оригинальной технологии SecuROM PA из защищенных игрушек (*Epic Mickey 2: The Power of Two*, *Grand Theft Auto IV*, *Bioshock* и др.). Навесная защита *VMProtect* навешана специально, дабы минимизировать появление «левых» модифицированных копий программы.

Если сгенерированный unlock code не принимается защитой. Ничего страшного нет! В 99,99999% случаях проблема в хэше серийного номера, который был уже использован и хранится в реестре у SecuROM. Для удаления использованных

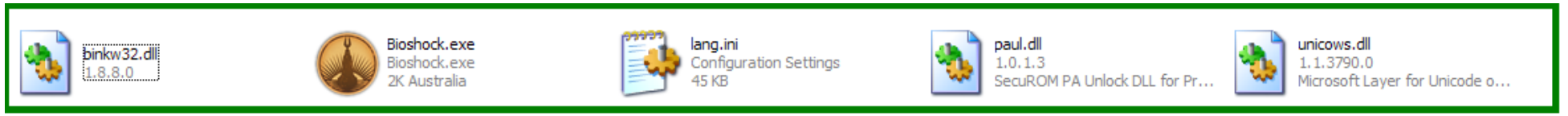
хэшей потребуется почистить определенную ветку реестра или можно зайти с другой стороны – просто задать в расширенных опциях (*[80_PA] Advanced*) другое значение *UC.Serial number stamp* в формате Hex (2 байта). Более подробно в пункте 3.

Если моей игры нет в списке «*Aviable KEY KITs*». К сожалению, к моменту выпуска 80_PA не удалось собрать полную базу защищенных игрушек, хотя общими усилиями удалось достать такие редкие игры, как *ys7 (ys seven)*. Но если Ваша игрушка, использующая технологию SecuROM PA, отсутствует в списке, то Вы можете помочь дополнить его! Пройдите в директорию установки игрушки, и соберите мин. рабочий набор, который должен включать в себя:

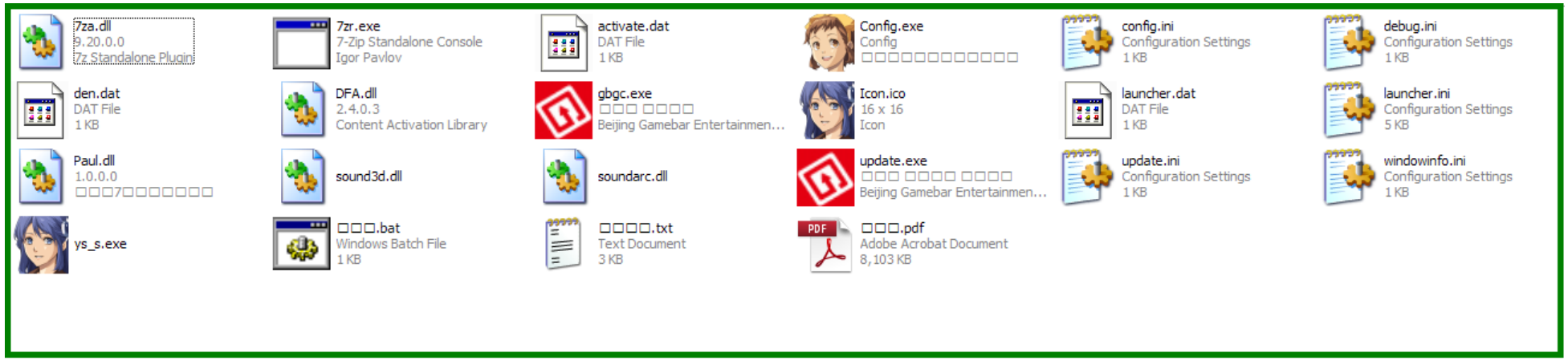
- **Главный .exe файл, который защищен SecuROM PA;**
- **PAUL.DLL, dfa, lang.ini** *(последние два, если есть)*;
- **Все возможные вспомогательные динамические .dll *(например,* binkw32.dll*)* в этой директории и .exe файлы;**
- **Различные мелкие .INI, .txt, и .dat файлы;**

Исключение составляют игры от компании «Telltale Games»: требуется оригинальный установщик игры (например, *Bone_Out_From_Boneville_Setup.exe*), ввиду специфического интерфейса, созданного для SecuROM PA.

Пример 1. BioShock:



Пример 2. Ys Seven:



Собрав указанные файлы воедино, заархивируйте в архив формата .zip или .7z (в сумме не должно получиться свыше 30 Мегабайт) залейте на файлообменник (рекомендуется www.wetransfer.com). Ссылку отправьте нам по почте (указана в контактах) или на сайте exelab.ru (cracklab.team). Наборы криптографических ключей будут выдраны и добавлены в библиотеку 80_PA!

Немножко долго идёт генерация unlock code и очень долго идёт декодирование unlock request code. ~~Даа! 😀 Мы немного схалтурили и не стали выдирать статический DES ключ в обоих случаях, пойдя по пути наименьшего сопротивления. Впрочем, если кто-то это готов сделать, дайте знать! Ваше имя будет занесено в список.~~
Пофикшено в версии v.2.0 (2020-2023)

АКТУАЛЬНА ЛИ ПРОДАЖА ИСХОДНЫХ КОДОВ SecuROM и DENUVO? Естественно, как никогда ранее. Свяжитесь со мной всеми доступными способами, предварительно написав в cracklab.team (exelab.ru). qTox – наиболее предпочтительный вариант! Доступен также *Telegram*. Исходные коды нужны исключительно для внутреннего исследования только одним человеком (мной).

Принудительное включение ручной (Manual) активации для игр с Trial-mode («*BigFish Games*») со сбросом.

Эпичный трюк:

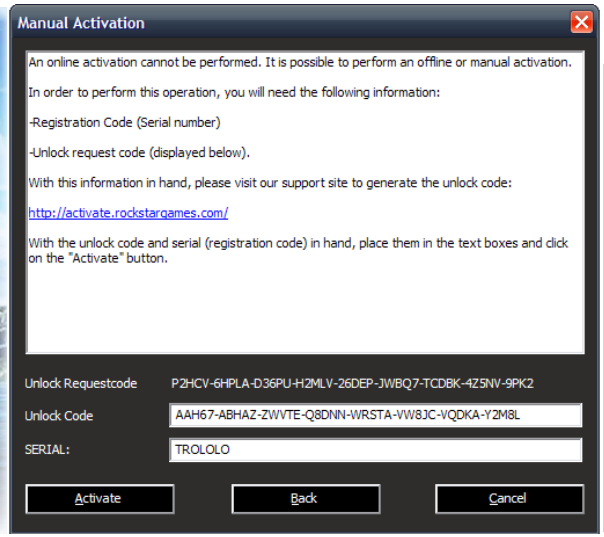
1. **Заменяем текущую новую версию paul.dll (обычно v2.x) в каталоге игрушки на древнюю версию paul.dll (v 1.x)**
2. **Получаем возможность «Manual activation» (активация вручную)!**
3. **Используем 80_PA**
4. **Сбрасываем в служебной структуре все три LOCK-бита (по дефолту, должны быть сброшены)**
5. **Генерируем свободный unlock code**
6. **Вставляем и активируем**
7. **PROFIT!!!**

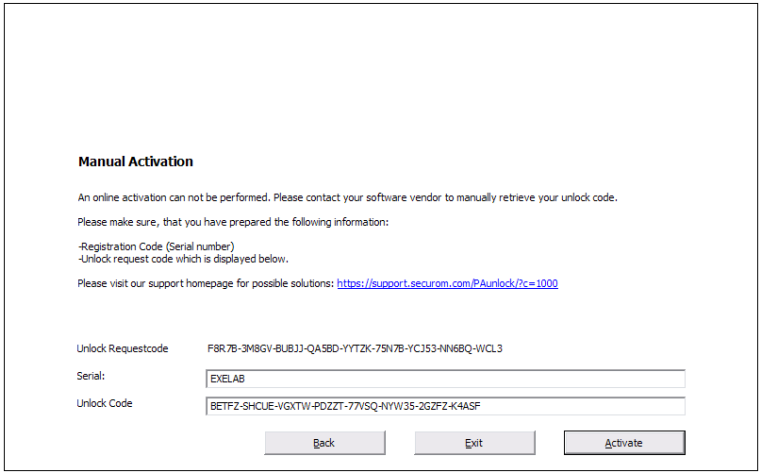
Принудительное удаление HKEY_CURRENT_USER\Software\SecuROM\License information и !CAUTION!. Просто нажмите кнопку «Hidden reg keys». Суть трюка в использовании недокументированных возможностей чтения/создания веток реестра с помощью низкоуровневых функций из ntdll и учета null-байта в конце имени ветки.

Про DENUVO и окончательный взлом SecuROM. Проект 80_PA является далеко не единственным достижением при исследовании SecuROM. По факту, были исследованы и взломаны почти все возможности SecuROM: начиная от банальной анти-отладки и заканчивая виртуальной машиной (virtual machine) с модулем проверки компакт-дисков. В последнем была найдена критическая уязвимость, которая затрагивает абсолютно все версии защиты и позволяет убийственным образом запускать защищенные программы без оригинального лицензионного компакт-диска и даже без традиционного Alcohol 120% с Daemon Tools! (https://xakep.ru/2015/08/07/securom/). Также велась работа над DENUVO - топик (https://exelab.ru/f/index.php?action=vthread&forum=13&topic=19719) является самым точным первоисточником информации об этой защите (не в пример лучше, чем у 3dm).

Краткое описание технологии онлайн-активации SecuROM. Терминология.







Терминология (глоссарий):

SecuROM PA (Product activation, online-activation)	Собственно оригинальная технология онлайн-активация SecuROM
SONY DADC AG	Компания, которая производила SecuROM
HWID (Hardware ID)	Уникальный идентификационный номер Вашего компьютера, который формируется из различных данных об установленном «железе». Каждая защита формирует его по своему индивидуальному алгоритму. Касаемо SecuROM, алгоритм генерации будет описан ниже.

MD5 (Message Digest 5)	128-битный алгоритм хеширования, разработанный профессором Рональдом Л. Ривестом из Массачусетского технологического института (Massachusetts Institute of Technology, MIT) в 1991 году. Предназначен для создания «отпечатков» или дайджестов сообщения произвольной длины и последующей проверки их подлинности
DES (data encryption standard)	Алгоритм для симметричного шифрования, разработанный фирмой IBM и утверждённый правительством США в 1977 году как официальный стандарт (FIPS 46-3). Размер блока для DES равен 64 бита. В основе алгоритма лежит сеть Фейстеля с 16-ю циклами (раундами) и ключом, имеющим длину 56 бит.
RSA (аббревиатура от фамилий Rivest, Shamir и Adleman)	Криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.
CRC (Cyclic redundancy check)	Циклический избыточный код - алгоритм нахождения контрольной суммы, предназначенный для проверки целостности данных.
XOR	Битовая операция (исключающее «ИЛИ»).
appid	Уникальный идентификатор (3 линии * 16 байт = 48 байт), который SecuROM присваивает любой игрушке.
Unlock requestcode	Код-запрос на сервер SONY DADC AG, содержащий зашифрованный HWID Вашей машины (RSA) и служебную структуру (DES), в которой содержится также CRC от MD5-хэша appid, для получения unlock code.
Unlock code	Код-ответ, сгенерированный сервером, по данным из unlock requestcode, но с другими ключами. В коде-ответе есть своя служебная структура (DES) и зашифрованный HWID (RSA). В

	служебной структуре unlock code учтён хэш серийного номера.
Serial (s/n или serial number)	Серийный номер, который обычно пишут на приобретенном лицензионном диске. Для сервера является гарантом того, что Вы являетесь покупателем диска. В реализации 80_PA вообще не требуется легально приобретенный серийный номер! Его дайджест будет сгенерирован от балды или введён Вами с потолка.
47 (0x2f)	Длина unlock code
52 (0x34)	Длина unlock requestcode
48 (0x30)	Длина appid
28 (0x1C)	Длина строчного HWID (ASCII)
16 (0x10)	Длина HWID в байтах

Вся процедура генерации делится условно на три этапа:

1. Генерация HWID, формирование unlock requestcode на машине пользователя с использованием appid;
2. Отправка unlock requestcode на сервер. Расшифровка и проверка на сервере unlock requestcode, при условии нахождения s/n в базе. Извлечение дайджеста appid и других служебных данных из requestcode, формирование unlockcode с использованием других ключей шифрования. Добавление LOCK-байт, если требуется. Отправка unlock code обратно на машину пользователя;
3. Получение unlock code. Расшифровка. Сверка дайджеста серийного номера с сохраненными ранее. Извлечение HWID из unlockcode и генерация HWID на текущей машине. Сверка двух полученных HWID по маске.
4. Условно. Проверка HWID при каждом запуске.
5. HWID состоит из хэшей над которыми применена логическая операция XOR:

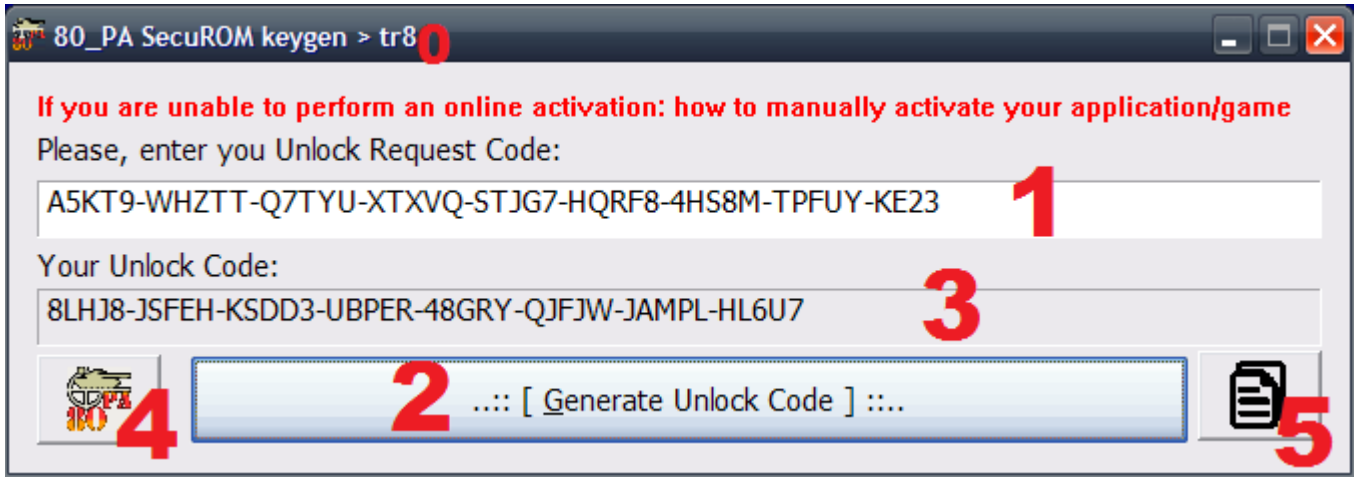
- Информации об операционной системе (WINAPI kernel32.GetVersionEx)*
- Информации об установленном процессоре (WINAPI kernel32.GetSystemInfo)*
- Информации об установленной видеокарте (WINAPI d3d9.Direct3DCreate9)*
- Информации об сетевой карте (WINAPI iphlpapi.GetAdaptersInfo)
- Информации о серийном номере системного тома, на котором установлен Windows (WINAPI kernel32.GetVolumeInformation)*
- Информации об остальных серийных номерах томов (WINAPI kernel32.GetVolumeInformation)

*Согласно маске, SecuROM проверяет только указанные хэши.

Начиная от Bioshock и заканчивая самыми последними защищенными игрушками, процедура активации одинакова байт в байт!!! Естественно, различия только в адресах, appid и специальных константах, которые используются для сверки результатов работы функций онлайн-активации. HWID будет различным на любой машине. После изменения Вашей конфигурации «железа» (например, Вы поменяли видеокарту), при следующем запуске SecuROM обнаружит несовпадение HWID, и активация потребуется заново. Также, хэш серийного номера будет занесен в «черный список», который можно нелегально очистить или же провести официальный отзыв ключа (revoke).

Процедура генерации правильного unlock code. Описание возможных ошибок и их устранение.

версия 2 (основная)

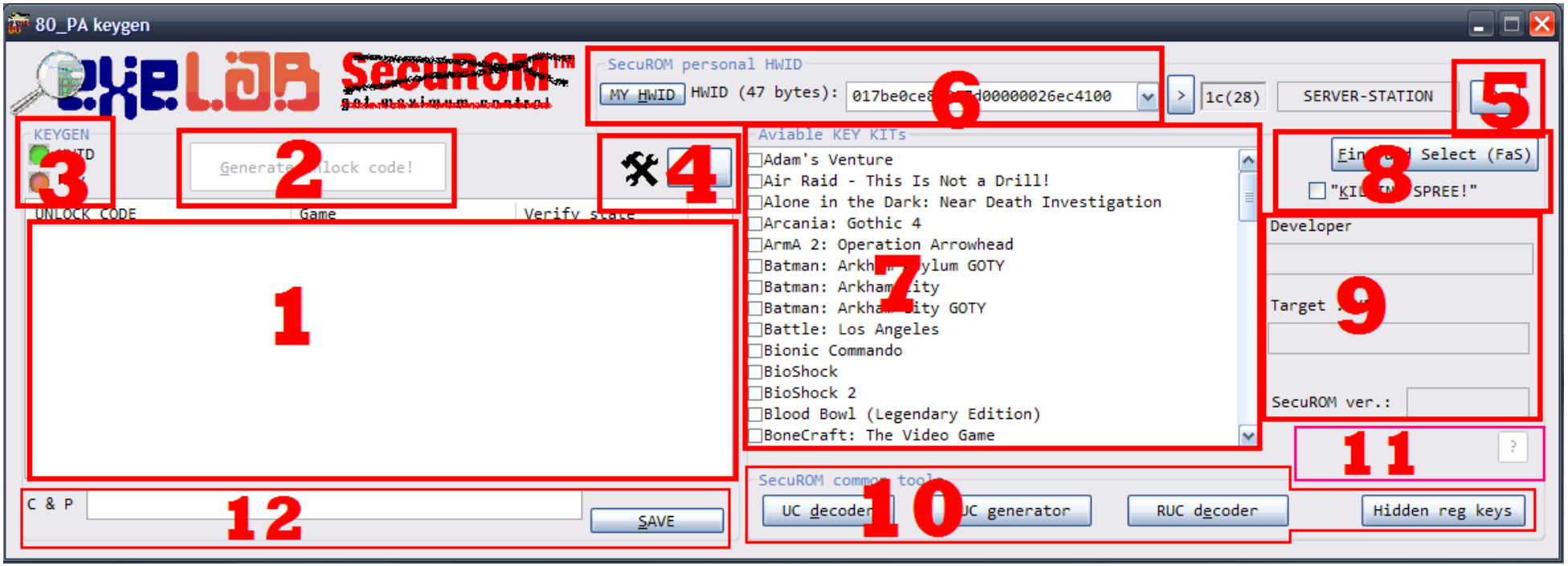


0. Автоматика может распознать заранее запущенную игру с SecuROM 7-8 (0). Например: Tomb Raider
1. Вводим REQUEST CODE (код запрос, длиннее кода-ответа) в поле (1)
2. Нажимаем «Generate Unlock Code» (сгенерировать код-ответ) используя кнопку (2)
3. Забираем готовые Unlock Code из поля ввода (3)
4. При необходимости вызываем предыдущую расширенную версию 80_PA кликнув на кнопку (4)
5. Копирование готового кода-ответа можно осуществить без помощи клавиатуры (Ctrl+C), нажав кнопку (5)

версия 1 (второстепенная)

6. Переход осуществляется из главного окна при нажатии кнопки слева внизу или вызове 80_PA.exe с любыми аргументами.

7. Первая версия программы выглядит следующим образом:



Легенда:

(1) ListBox, в котором отображаются сгенерированные unlock code;

(2) Кнопка «Generate unlock code», которая, собственно, запускает процесс генерации;

(3) Контрольные лампы: валидность HWID и выбранный набор ключей (игры);

(4) Расширенные опции генерации (ключевые значения сервисной части unlock code, параметры криптографии)

(5) Расширенная информация по SecuROM HWID

(6) Текущее значение SecuROM HWID (изначально соответствует Вашему персональному HWID). Можно менять по своему усмотрению.

(7) Доступные наборы криптографических ключей (appid, DES, RSA) для генерации – перечень игр.

(8) Опция «Find and Select» («найти и выбрать») – ищет в запущенных процессах по имени файла из KEY KITs игры с технологией SecuROM PA. Значительно упрощает нахождение правильного набора ключей для генерации. Рядом находится CheckBox «Killing spree!» (Серия убийств) – выбирает все доступные наборы ключей (игр). Повторное нажатие снимает выделения.

(9) Информация о выбранной игре (разработчик, имя целевого файла .exe, версия защиты SecuROM)

(10) «UC Decoder» - декодер unlock code. Можно самостоятельно проверить структуру сгенерированного unlock code. «RUC Generator» - генератор request unlock code. Нужен для формирования фиктивного request unlock code при отправке запроса на официальные сервера активации SecuROM PA. «RUC Decoder» - декодер request unlock code. «Hidden reg keys» - даёт возможность просмотра и удаления недоступных веток *\HKCU\SOFTWARE\SecuROM\License information* и *\HKCU\SOFTWARE\SecuROM\!CAUTION! NEVER DELETE OR CHANGE ANY KEY*

(11) Панель пиктограмм. Подсвечивает важные замечания по игре (в части требований замены библиотеки-обвертки paul.dll и lang.ini из прилагаемых архивов в папке «80_PA addons» официального набора кейгена 80_PA, а также информацию о возможном использовании технологии «EA Game Authorization Management»). Детальную информацию можно получить, кликнув на кнопку «?», расположенную рядом с пиктограммами

(12) Последний сгенерированный unlock code будет вставлен в TextBox. Вы можете так же кликнуть на любой сгенерированный unlock code в ListBox (указанный в пункте 1), для удобного копирования строки unlock code. Кнопка «Save» сформирует отчет из всех сгенерированных unlock code и сохранит его на диск в любом указанном Вами месте.

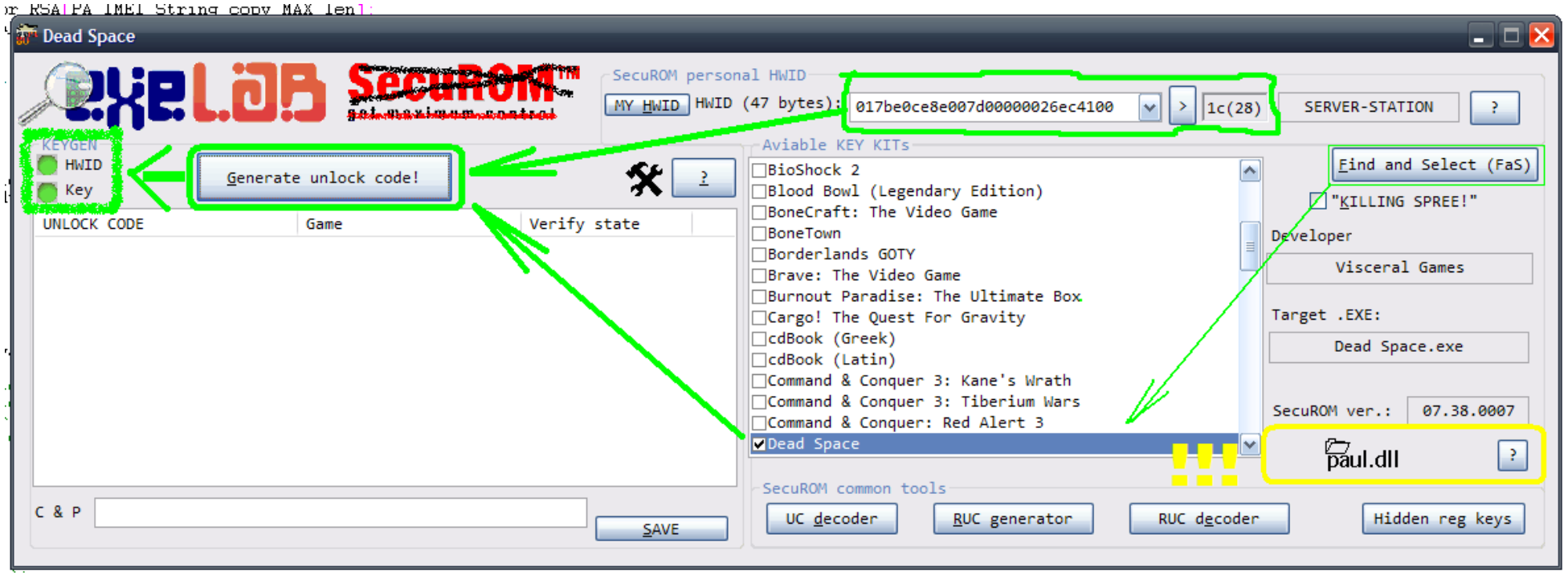
8. Определяемся с игрушкой, для которой нужно сгенерировать unlock code. Здесь есть три варианта:

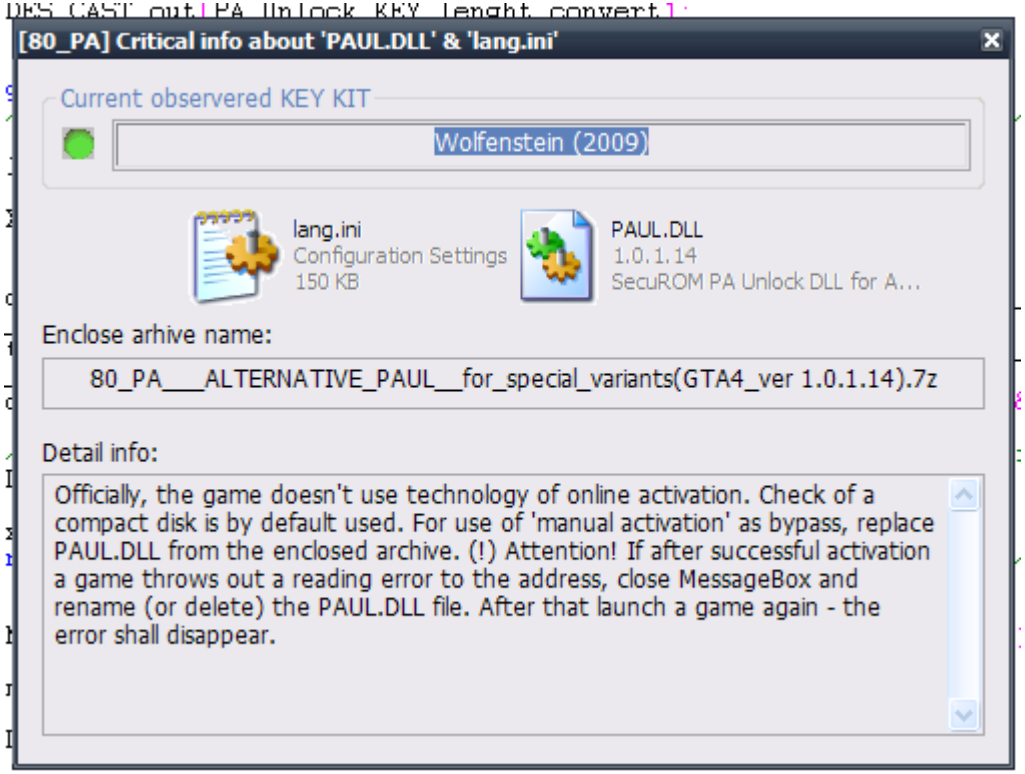
a) Выбираем требуемое количество игрушек вручную в списке (7) – ставятся галочки;

b) Если игра запущена и активно окошко SecuROM manual-activation, то просто задействуем опцию «FaS» (8). В шапке главного окна при этом будет отображаться название выбранной игры или же, в противном случае, будет указано, что ничего не найдено («FaS – Nothing found»)

c) Выбираем «Killing spree!», чтобы сгенерировать unlock code для всех доступных игрушек в библиотеке 80_PA;

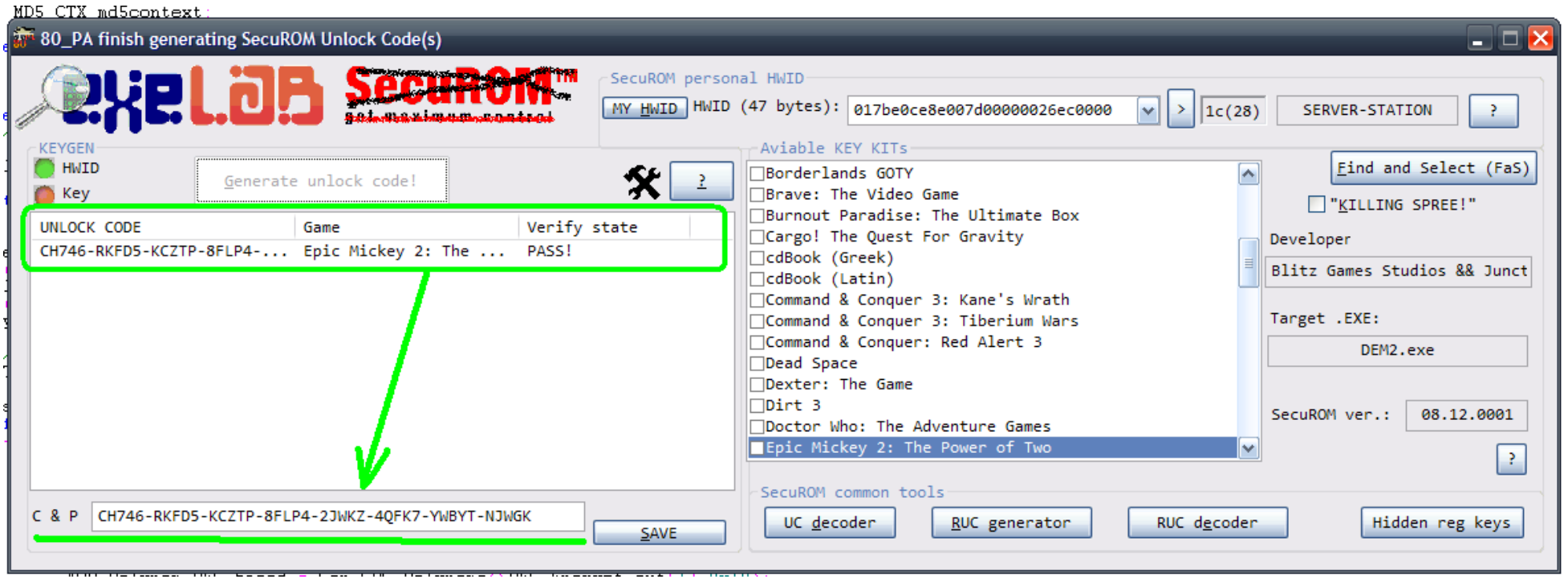
9. Убеждаемся, что все две контрольные лампы (3) горят зеленым цветом. Это является указанием для разблокировки кнопки запуска генерации (2). Обратите внимание так же на пиктограммы, обведенные желтым цветом – возможно, Вам понадобится выполнить дополнительные операции с файлами paul.dll (Product Activation Unlock Library. Dynamic Link Library) и lang.ini (Language). Архивы (в формате .7z) с названными файлами входят в официальный комплект 80_PA и расположены в папке с названием 80_PA addons



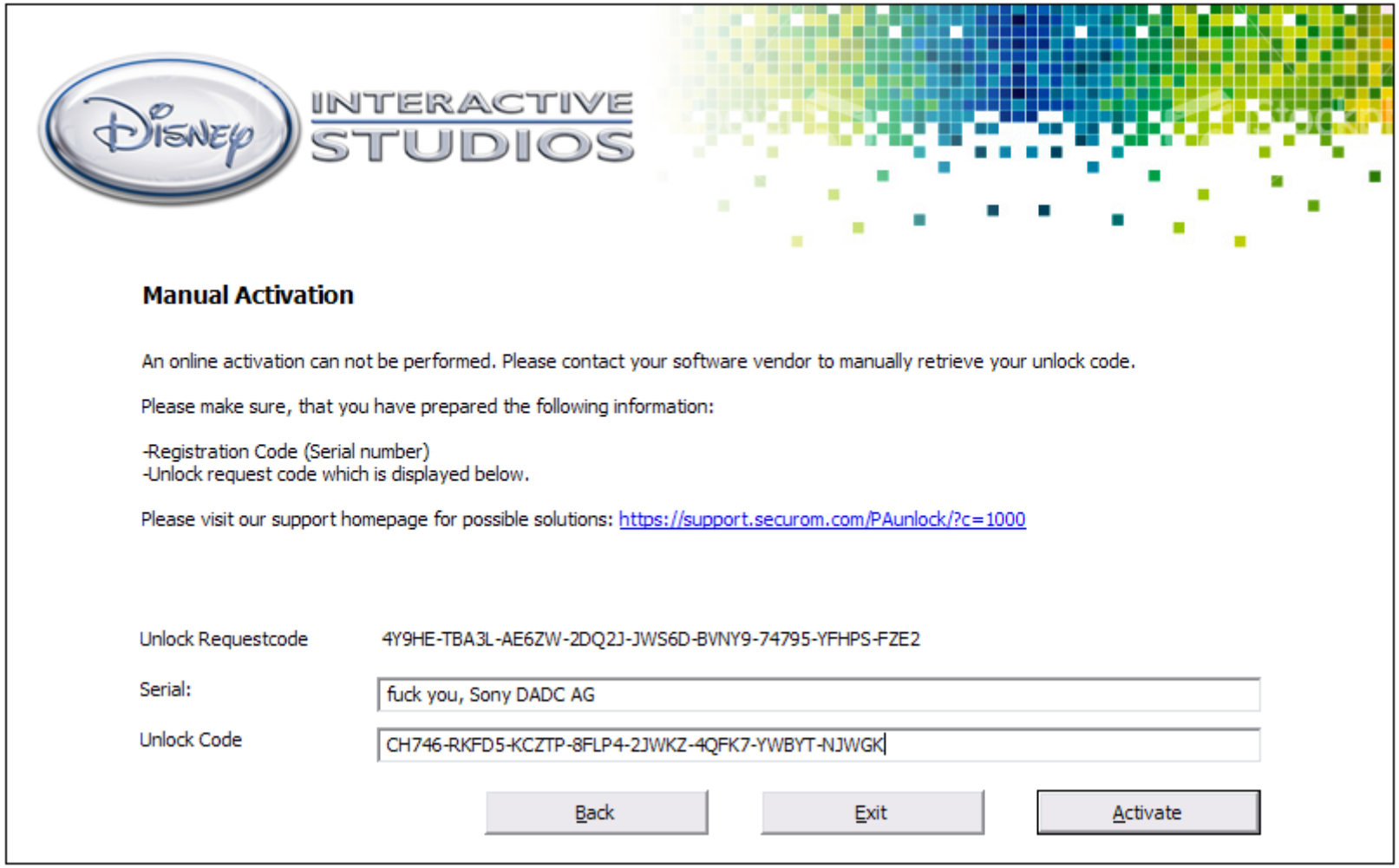


10. **Нажимаем кнопку (2), шапка главного примет сообщение «80_PA start generating SecuROM Unlock Code(s)» и ждем некоторое время (в зависимости от мощности процессора и количества выбранных игр);**

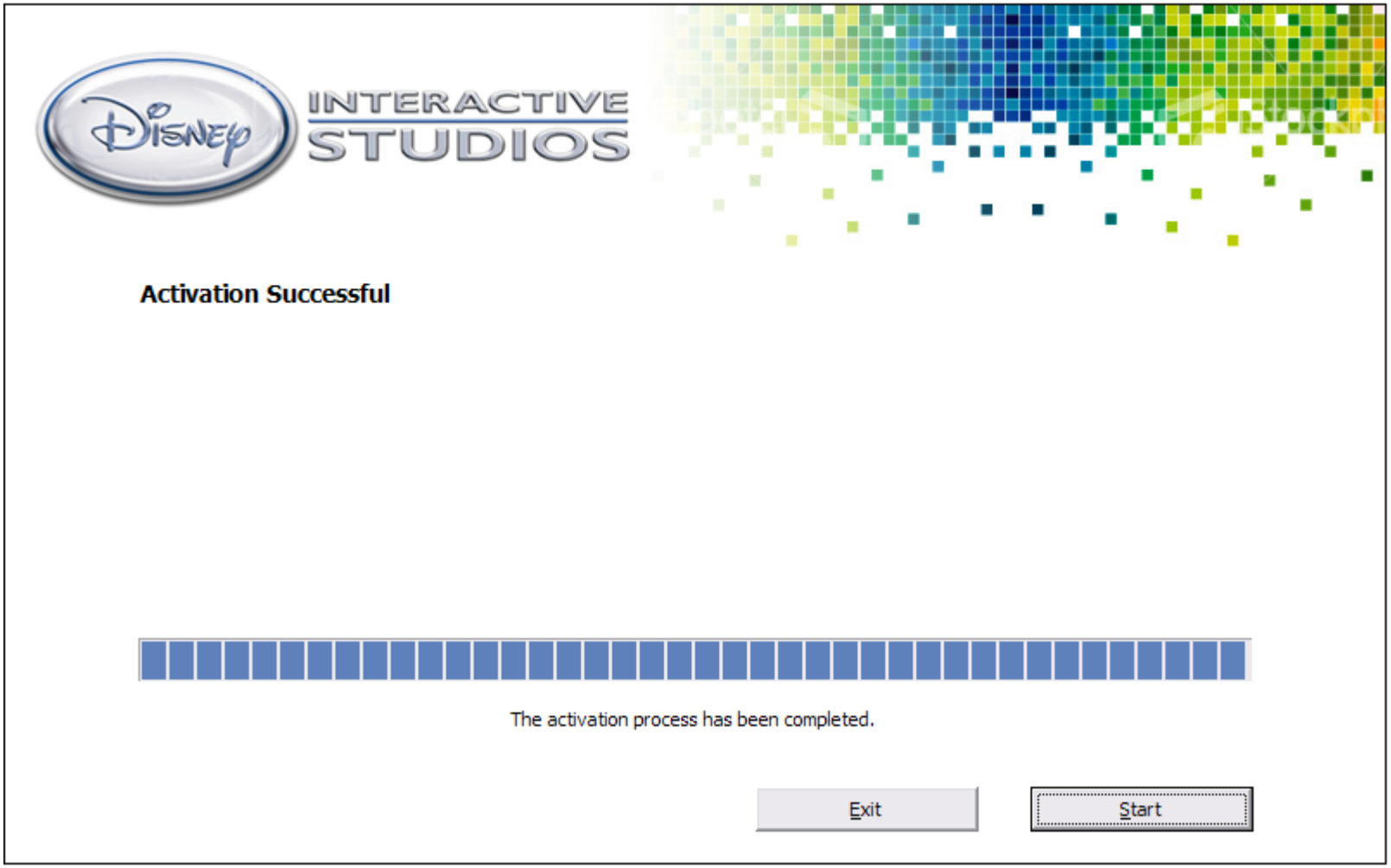
11. Дожидаемся окончания генерации unlock code. Впрочем, при множественном выборе 80_PA периодически будет добавлять сгенерированные данные в список, и ими можно будет пользоваться. Последний сгенерированный unlock code отображается в поле ввода EditBox C & P (Copy & Paste) откуда можно без проблем скопировать код-ответ. Выбирать код-ответ для копирования можно в списке выше, щелкнув правой кнопкой мыши. Полное окончание генерации будет ознаменовано сообщением в шапке главного окна «80_PA finish generating SecuROM Unlock Code(s)». Колонка «Verify state» (статус проверки) отображает результат проверки unlock code по алгоритму, заложенному в защищенных файлах SecuROM PA («PASS!» – проверка пройдена полностью; «Invalid HWID part» - все две стадии распаковки unlock code пройдены, однако полученный HWID не совпадает с HWID Вашей машины; «UC not unpack» - unlock code невозможно распаковать на первой стадии получения его служебной части)



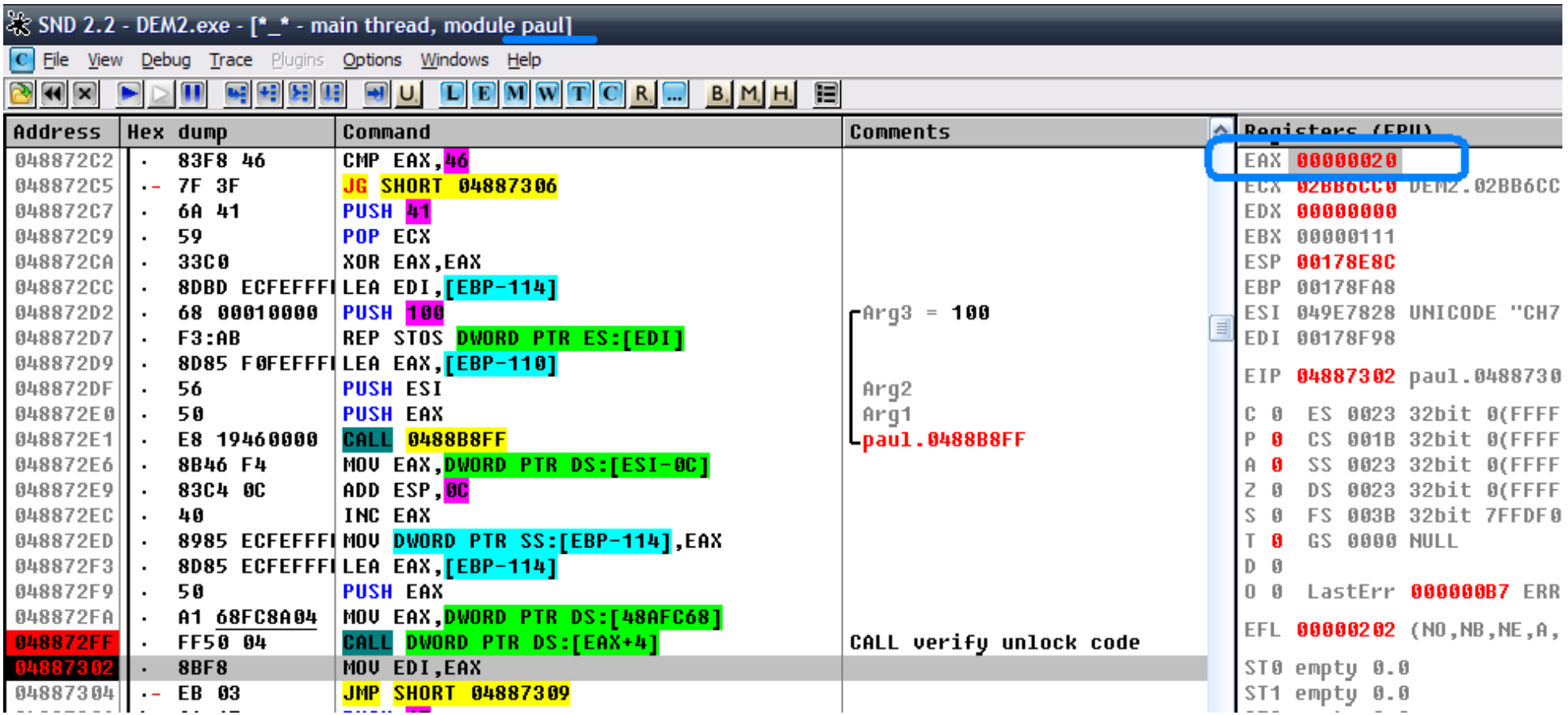
12. Вставляем сгенерированный unlock code в соответствующее поле ввода окна «Manual activation». В поле ввода Serial вводим любую белиберду (фигню, бред, ерунду, хрень, с потолка, от фонаря и тд). Нажимаем кнопку «Activate»!



13. Если всё сделано было правильно, то в идеальном варианте Вы должны увидеть заветное «Activation Successful». Нажимаете «Start» и спокойно играете… до того момента, когда лицензия SecuROM PA может быть потеряна из-за установки нового «железа» или слёта видеодрайверов.



14. Если активация завершилась с ошибкой, и Вы читаете этот пункт. Актуально для ранних версий 80_PA, в ver2.0 такое нереально. В самом крайнем случае, нужно сгенерировать unlock code повторно. Тем не менее, во-первых, паниковать не стоит! Если Вы прошареный хакер-программист, то можете точно узнать код ошибки, заглянув в программу отладчиком – банально установите точку останова после вызова динамической библиотекой-обверткой paul.dll процедуры проверки unlock code. В 32битном регистре процессора EAX будет отображаться код ошибки. Допустим в ~~OllyDbg~~ SND 2.2 это будет выглядеть так:



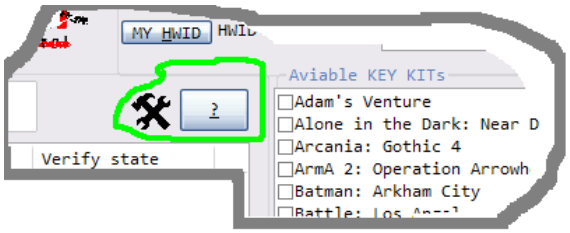
В данном случае код 0x20 говорит о том, что дайджест серийного номера (serial) находится в черном списке в локальном хранилище SecuROM PA. Это самая распространенная ошибка в процессе активации.

Ниже приведена таблица наиболее часто встречающихся кодов ошибок.

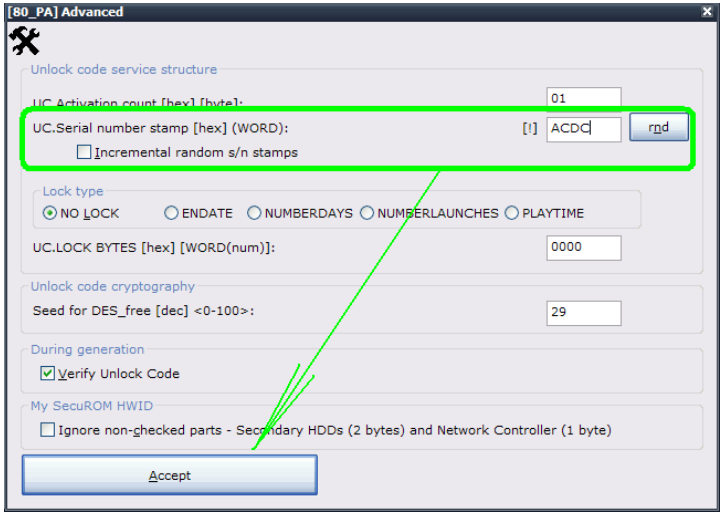
Часто встречаемые коды ошибок, возвращаемых процедурой проверки unlock code		
Код ошибки в регистре EAX после вызова (HEX-формат)	Условный макрос / соответствие в 80_PA	Описание
1	**PA_ERROR_SUCCESS**	**Активация проведена успешно**
7	PA_ERROR_UNLOCK_LEN_MISMATCH	**Длина строки unlock code не равна 47 байтам**
9	PA_ERROR_IMEI_PART_NOT_VALIDATE **«Invalid HWID part»**	**Не распакована (не сходится) HWID (IMEI) часть unlock code.** ***Вероятная причина:*** **полученный HWID из unlock code не совпадает с Вашим машинным.**
0x14	PA_ERROR_UNLOCK_SERVICE_PART_NOT_VALIDATE **«UC not unpack»**	**Не распакована служебная часть unlock code.** ***Вероятные причины:*** **не подходит ни один seed из диапазона 0-100 для рандомного набора DES** или **сформированный из индивидуального appid, дайджест не совпадает с прописанным дайджестом в служебной части unlock code** (перепутаны unlock code).
0x20	**PA_ERROR_SERIAL_DIGEST_BLACK_LIST**	**Дайджест серийного номера (serial) находится в черном списке в локальном хранилище SecuROM PA**

Если же Вы не владеете техникой отладки, тогда ничего страшного также нет. В 99,9999% случаев ошибка будет именно PA_ERROR_SERIAL_DIGEST_BLACK_LIST (дайджест серийного номера локально забанен защитой). Рассмотрим несколько вариантов решения данного недоразумения:

I. **Самый простой и быстрый, с использованием 80_PA.** Собственно, самое очевидное, что можно сделать – изменить дайджест серийного номера (2 байта) в генерируемом unlock code. Для этого пройдите в расширенные опции 80_PA(пиктограмма «ключ и молоток»). Сама кнопка выделена ярко-зеленым цветом:



Открывается вспомогательное окно «*[80_PA] Advanced*». В группе «Unlock code service structure» меняем значение «UC.Serial number stamp» на отличное от предыдущего. Рекомендуется воспользоваться кнопкой «rnd» для генерации случайного значения. Возможно так же назначить галочку для *Incremental random s/n stamps*, для генерирования нового значения индивидуально для каждого unlock code в течении текущей сессии. Утверждаем и сохраняем новое значение с помощью кнопки «Accept»



Повторяем генерацию unlock code с новым дайджестом серийного номера. Сгенерированный unlock code будет буквами/цифрами от старого.

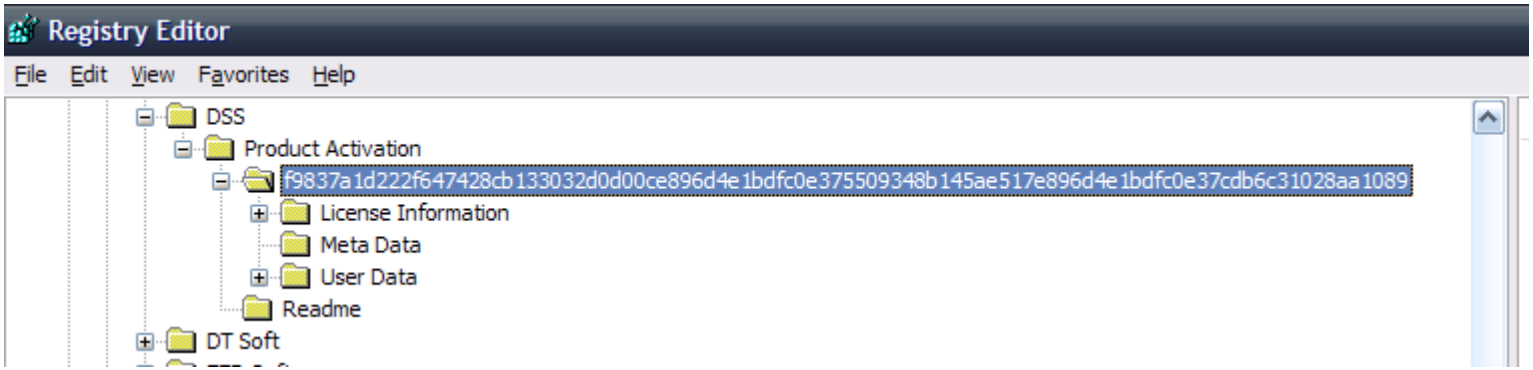
II. **Официальный отзыв лицензии (revoke), как способ сбросить черный список.** Используя ключ /revoke для 8й версии SecuROM и поздних 7х версий можно добиться очистки «черного списка» дайджестов серийных номеров. Для первых версий необходимо качать спец. программу revoke.

III. **Неофициальное (прямое) удаление лицензии SecuROM PA для 8й версии SecuROM (для продвинутых).** Для этого необходимо воспользоваться редактором реестра Windows (например, стандартный regedit) и знать уникальный appid для каждой игрушки (его можно вытащить с помощью отладчика). Здесь, для каждой игрушки в реестре будет свой «черный список» дайджестов серийного номера.

Заходим. Место назначения – ветка активации SecuROM PA: HKEY_CURRENT_USER\Software\DSS\Product Activation\

В данном случае, мы находимся в ветке игрушки «*Epic Mickey 2: The Power of Two*», HWID для которой равен

f9837a1d222f647428cb133032d0d00ce896d4e1bdfc0e375509348b145ae517e896d4e1bdfc0e37cdb6c31028aa1089



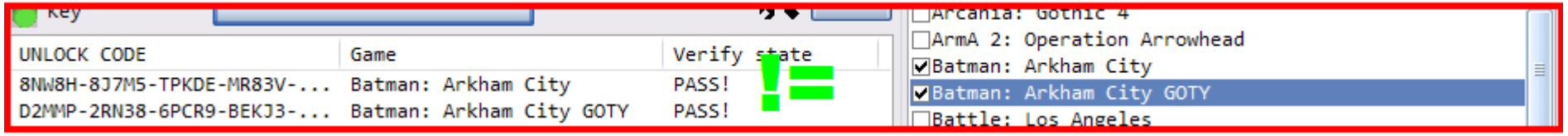
Удаляем указанную ветку, тем самым сбрасывая лицензию. Если Вы удалите корневую ветку HKEY_CURRENT_USER\Software\, то сбросятся лицензии для всех игр.

15. Повторяем процедуру регистрации *(при наличии ошибок!)*.

Особые замечания по следующим играм

1. **«Ys Foliage Ocean in Celceta». Для взвода «Manual activation» замените в папке с игрой динамическую библиотеку paul.dll и добавьте lang.ini из архива** *80_PA___ALTERNATIVE_PAUL__for_ysc (ver 2.0.1.3).7z*

2. **GOTY (Game Of The Year) edition. Обратите внимание, что одни и те же игры могут различаться по исполнениям и соответственно иметь разные наборы ключей.**



3. **(Trial mode) «The Travels of Marco Polo», «Sir Pudding Wiggly». Для взвода «Manual activation» замените в папке с игрой динамическую библиотеку paul.dll и добавьте lang.ini из архива** *80_PA___ALTERNATIVE_PAUL__for_defeat_TRIAL_MODE and EA (ver 1.0.1.3).7z*

4. **(EA Game Authorization Management) «Command & Conquer: Red Alert 3», «Mass Effect», «Spore», «The Godfather II», «Mirror's Edge», «Mercenaries 2: World in Flames», «Burnout Paradise: The Ultimate Box», «Sims 3». Для взвода «Manual activation» замените в папке с игрой динамическую библиотеку paul.dll и добавьте lang.ini из архива** *80_PA___ALTERNATIVE_PAUL__for_defeat_TRIAL_MODE and EA (ver 1.0.1.3).7z*



5. **(Региональная разбивка) «TRON: Evolution»** и **«TRON: Evolution (RUSSIAN)». Обратите внимание, что одни и те же игры могут различаться также по региональным признакам и соответственно иметь разные наборы ключей (аналогично, как в случае с GOTY edition).**

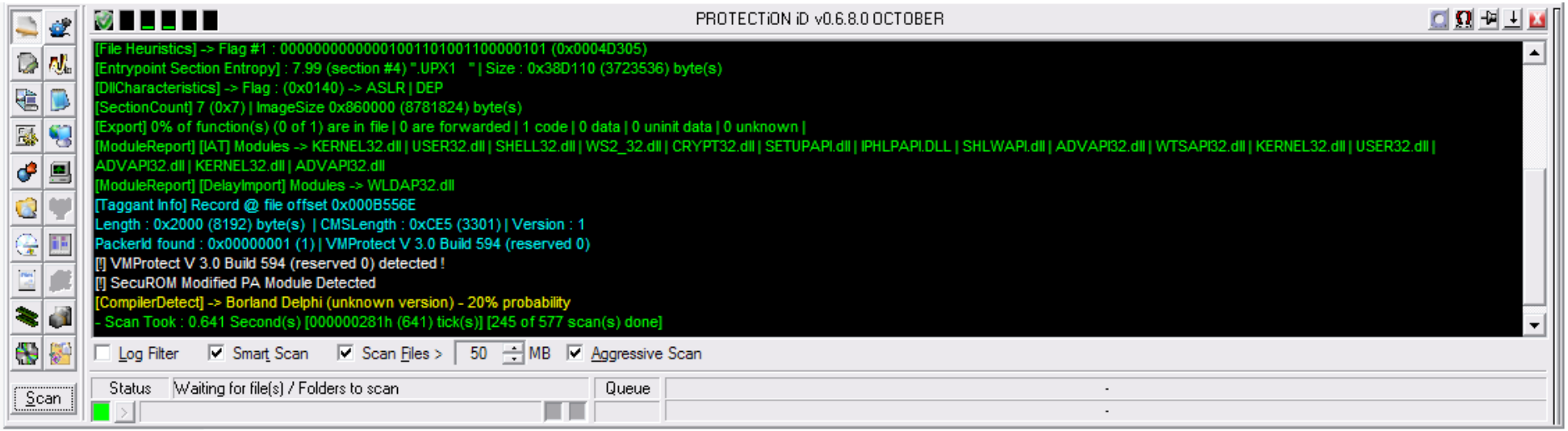
6. **(Особые ситуации) «GTA IV». Некоторые пользователи указывали, что при успешно завершенной активации игра требует вставить лицензионный компакт-диск в привод. В настоящий момент, при взломе SecuROM мы не наблюдали подобной ситуации. Обычно в защите установлено условие ИЛИ, т.е. или онлайн-активация, или компакт-диск. Впрочем, Вы можете ознакомиться с документом *Sony DADC SecuROM vulnerability.pdf* для использования уязвимости в модуле проверки компакт-дисков SecuROM. «GTA IV EFLC». Для EFLC нет никакой разницы при запуске исполняемых файлов LaunchEFLC.exe или SteamActivation.exe (Steam) – в обоих случаях наборы ключей одинаковы.**

7. (Версия 08.13.xx – новейшие, но малоизвестные игры 2016 г.) «Tale of Wuxia: Prequel» (с учетом обновления от 17/10/16). Для взвода «Manual activation» замените в папке с игрой динамическую библиотеку paul.dll и добавьте lang.ini из архива *80_PA___ALTERNATIVE_PAUL__for_ysc (ver 2.0.1.3).7z*. Необходимо отметить, что для данной версии SecuROM PA частично изменен код процедуры активации - рекомендуется удалить/переименовать файлы active.exe и deactive.exe, находящейся в папке с игрой. В частности особые изменения коснулись алгоритма RSA:

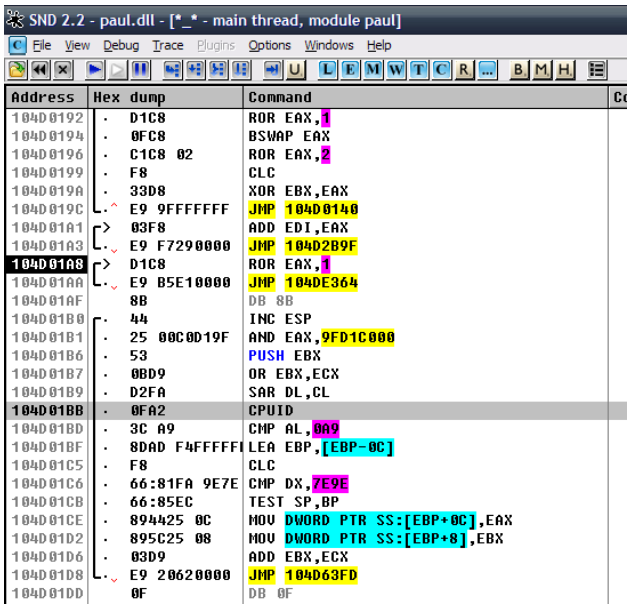
7.1 модуль *n* (аргумент №4) теперь передается в искаженном виде. Непосредственно правильный модуль формируется в самой процедуре RSA. Предполагается как: y = x^e mod (n*const)

7.2 входной шифротекст «ciphertext» *x* (аргумент №2) и открытая экспонента *e* (аргумент №3) поменялись местами между собой. В тоже время, открытая экспонента *e* более берется не из аргумента №2, а находится непосредственно в теле алгоритма RSA (заинлайнена).

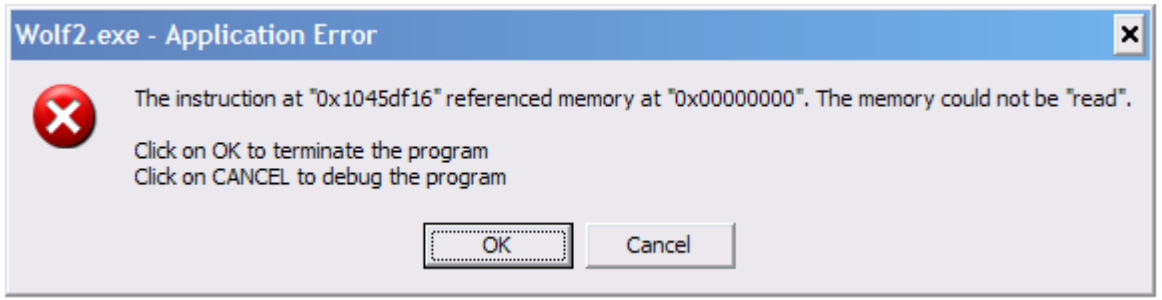
7.3 paul.dll, поставляемый с этой игрой, занимает 3,733,568 байт (почти 4 мегабайта). Есть основания утверждать, что paul.dll в этой версии упакован DENUVO x86 (VMProtect 3.0 + SecuROM). Результаты сканирования утилитой ProtectionIDv0.6.8.0(OCTOBER,2016):



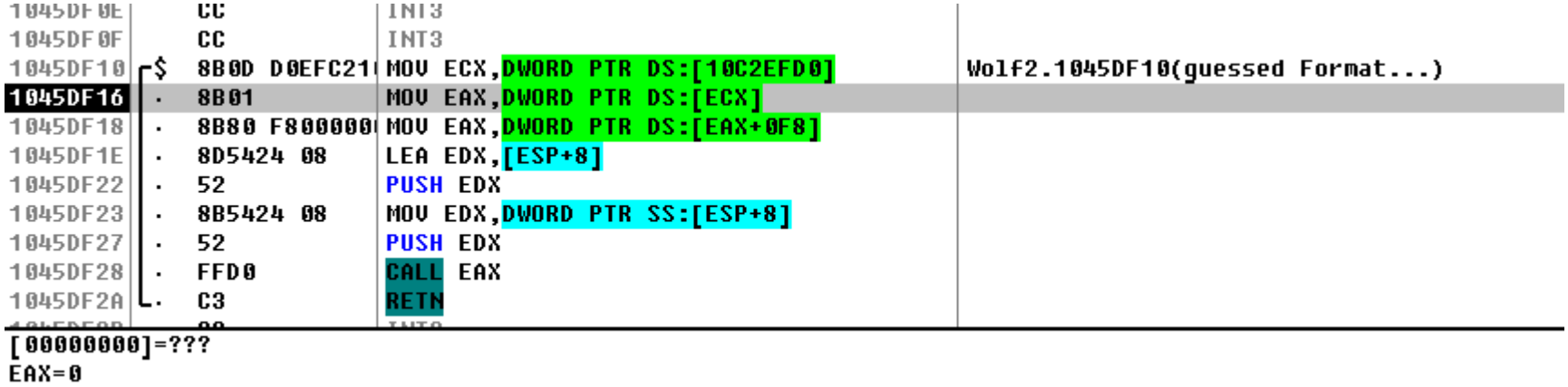
При отладке этой версии paul.dll часто встречаются инструкции CPUID, а также видна характерная обфускация:



8. **(Игры, официально не использующие онлайн-активацию. По умолчанию, взведена проверка лицензионного компакт-диска) «Dead Space», «Need for Speed: ProStreet», «Command & Conquer 3: Tiberium Wars», «Pro Evolution Soccer 2014», «Brave: The Video Game», «Lego Pirates of the Caribbean: The Video Game», «Operation Flashpoint: Red River». Несмотря на отсутствие файла-обвертки paul.dll в папке с указанными играми и появление диалога проверки компакт диска при запуске, существует неочевидный вариант использования 80_PA в качестве альтернативы проверки лицензионного компакт-диска. Все необходимые криптографические наборы уже зашиты в игру. Предположительно под данную уязвимость попадают все игры с версиями защиты >= 7.3x (вероятно есть связь между разработанной, в это же время виртуальной машиной и технологией онлайн-активации SecuROM PA). Для взвода «Manual activation» скопируйте в папку с игрой динамическую библиотеку paul.dll и lang.ini из архива *80_PA___ALTERNATIVE_PAUL__for_special_variants(GTA4_ver 1.0.1.14).7z* (в некоторых случаях допускается использование архива *80_PA___ALTERNATIVE_PAUL__for_defeat_TRIAL_MODE and EA (ver 1.0.1.3).7z*).**
9. **(Игры, официально не использующие онлайн-активацию. По умолчанию, взведена проверка лицензионного компакт-диска. Особый случай!). «Wolfenstein (2009)» (Версия игры: 0.91.25.7022). Для взвода «Manual activation» скопируйте в папку с игрой динамическую библиотеку paul.dll и lang.ini из архива *80_PA___ALTERNATIVE_PAUL__for_special_variants(GTA4_ver 1.0.1.14).7z*. Активируйте игру с помощью 80_PA. Если после активации появляется стандартное Windows сообщение «Application error» сообщающие об ошибке чтения по адресу:**



(В отладчике можно наблюдать это в указанном ниже месте)



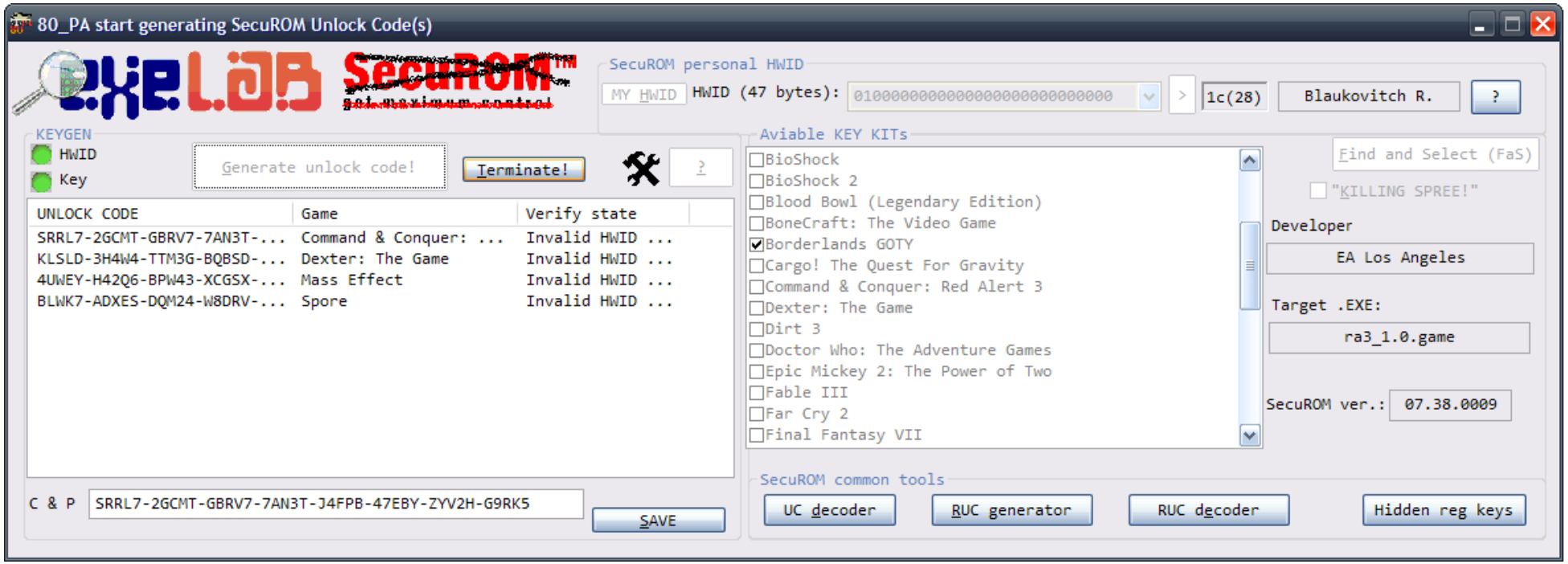
Решение: закройте MessageBox и переименуйте (или удалите) paul.dll в папке с игрой. Запустите Wolf2.exe снова – ошибка должна исчезнуть. Проверка лицензионного компакт-диска при корректной активации будет не активна.

10. (Игры от Telltale Games). Используют встроенную реализацию (built-in) API из paul.dll. Игнорируют внешний файл указанной библиотеки. Элементы интерфейса при активации отрисовываются при помощи встроенного браузера.

11. http://joyoland.com/, 北京欢乐百世科技有限公司, Nightshade (百花百狼), Norn9 (命運九重奏), Empire of Angels IV (天使帝國四), The Legend of Heroes: Trails from Zero (《零之轨迹》), The Legend of Heroes: Trails to Azure (英雄伝説 碧の軌跡：改), YS7 (イソ7), YSC (イース セルセタの樹海) Для исключения окна ввода имени пользователя и пароля (enter username & password), а так-же «введите действующий серийный номер» замените PAUL.DLL (DENUVO Gmbg) и lang.ini на более ранние версии из папки /80_PA addons в комплекте с 80_PA кейгеном. Это самые крайние версии SecuROM 08.13.076 (2018 год).

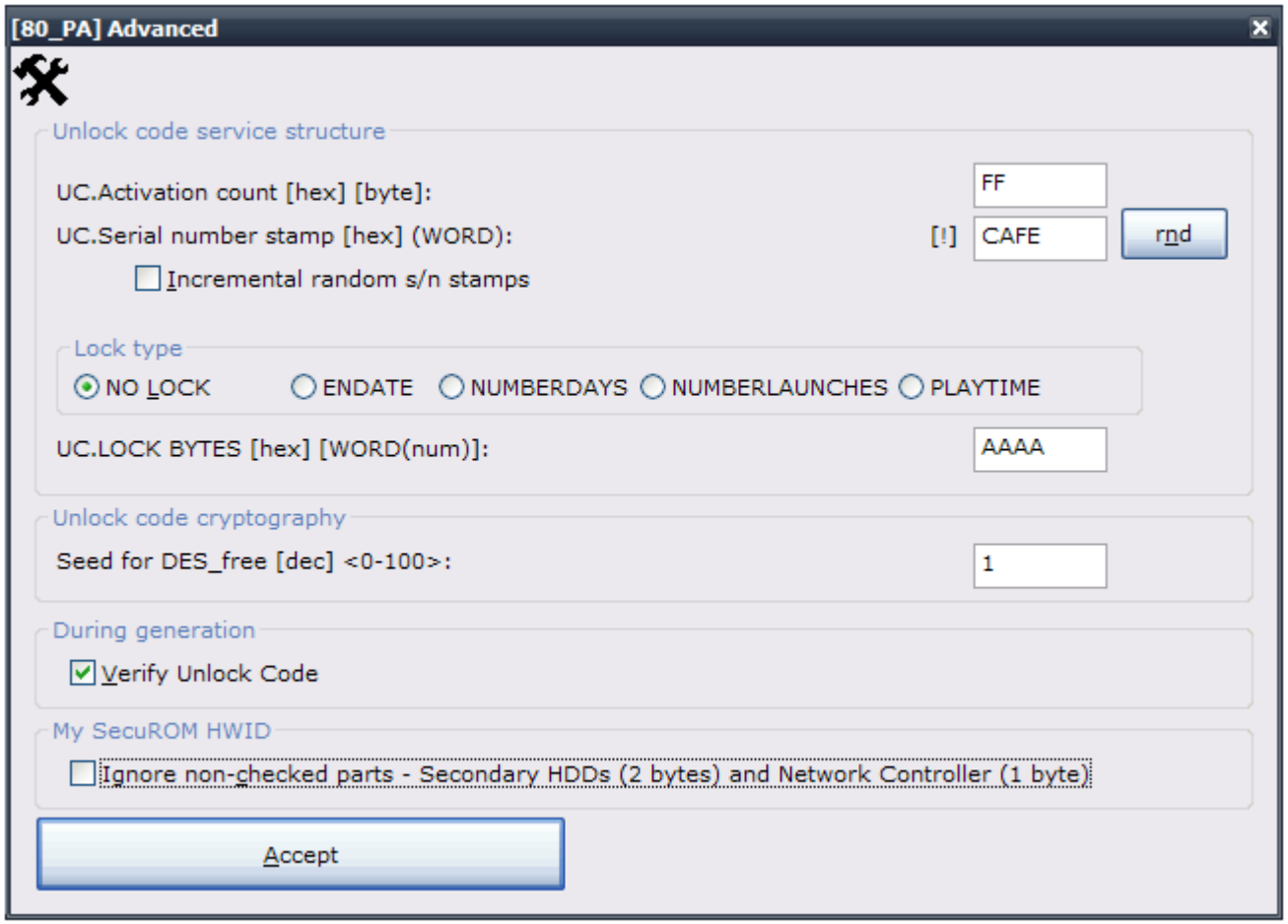
Проводник по окнам.

Второстепенное окно программы 80_PA. Здесь происходит генерация unlock code для выбранных игрушек. Отображается активный HWID. Осуществляется доступ к остальным окнам.



Опции, напрямую влияющие на конечный unlock code, показаны в окне [80_PA]Advanced

Рекомендуется изменять значение только в графе Serial number stamp



UC.Activation count – вероятно, количество активаций на Вашем HWID в базе данных сервера Sony DADC AG. Служит только для информации.

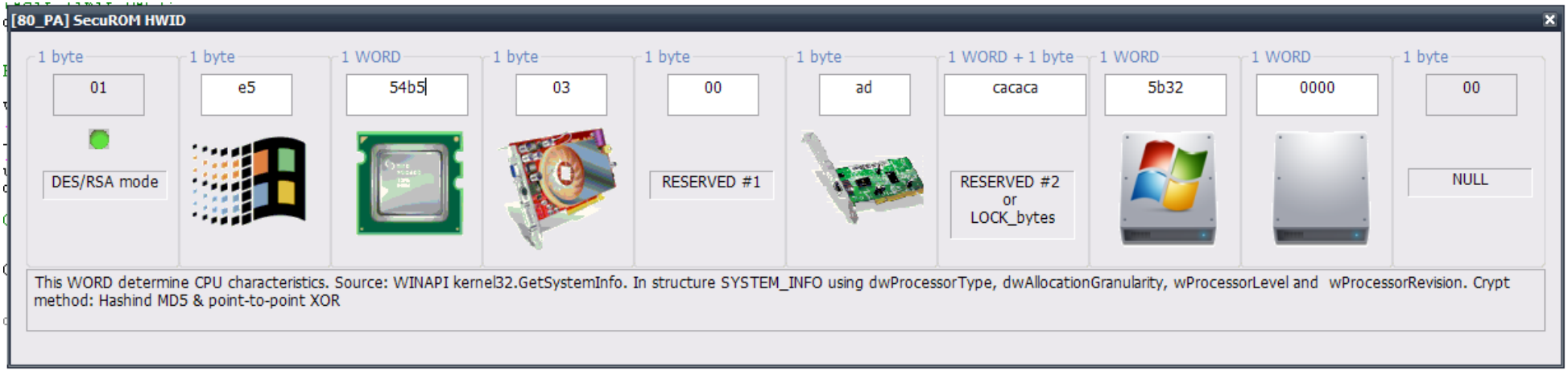
Lock type – тип блокировки с привязкой по количеству в **UC.LOCK BYTES**. Всегда взводите данный параметр как **NO LOCK**, иначе unlock code наложит ограничения на запуск.

Seed for DES_free – рандомно генерируемый seed для первичного (free) ключа DES. Величина seed влияет разве что на скорость перебора в цикле при расшифровке unlock code (чем больше значение – тем на одну итерацию больше).

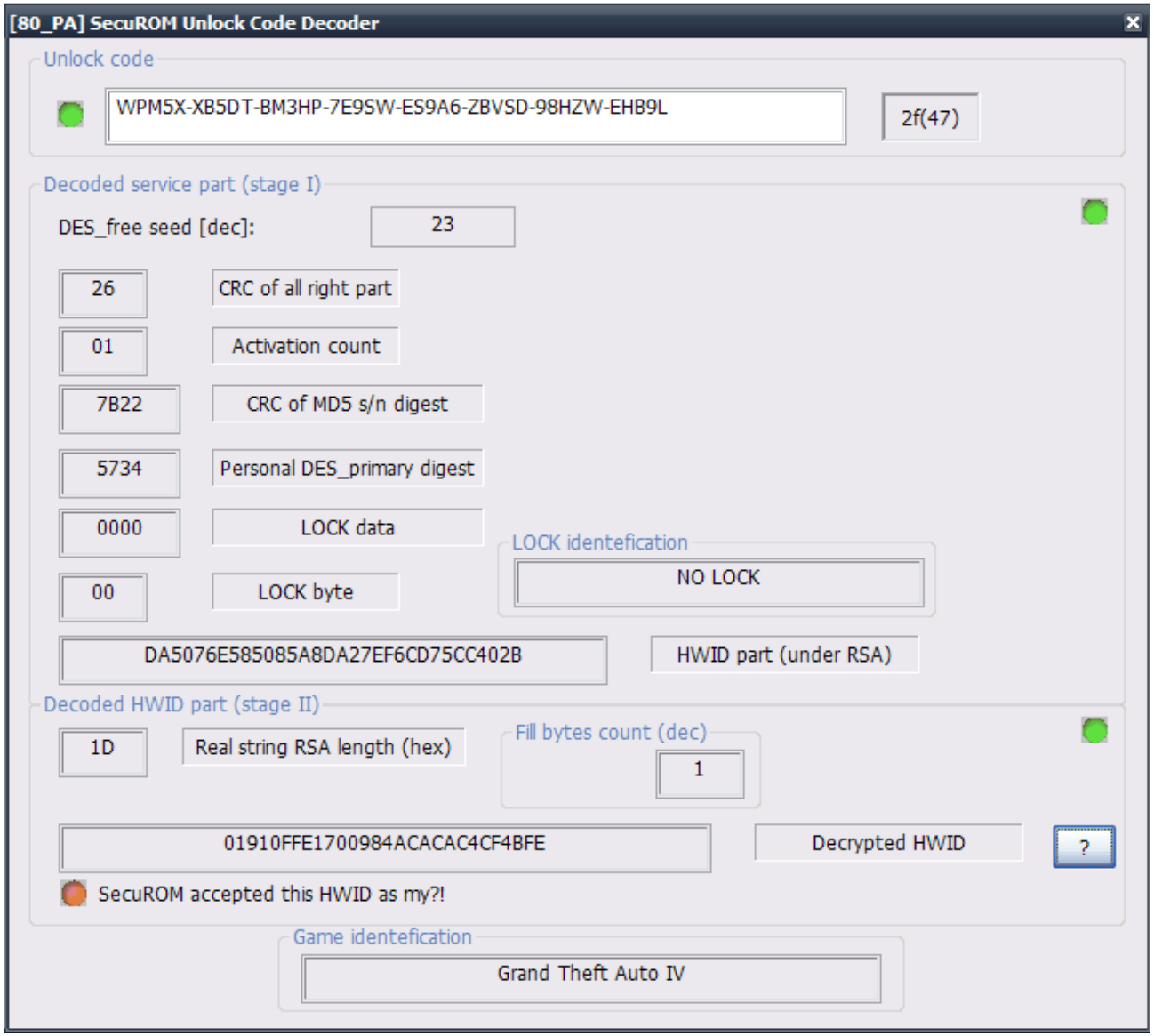
Ignore non-checked parts - Secondary HDDs (2 bytes)* and Network Controller (1 byte) – принудительно не вычислять хэши компонентов SecuROM HWID, которые влияют на конечный результат активации. В данном случае речь идёт о pa_raw_hwid. Network_nfo_hashik и pa_raw_hwid. Secondary_HardDisks_serial_nfo_hashik. Во всех исследованных играх, SecuROM не считает изменение данных значений, как нарушение лицензионной онлайн-активации. Допустим, в случае хэша Network_nfo_hashik (данные сетевой карты) изменение может произойти при обычном включении или выключении сети пользователем, т.е. факт смены самой сетевой карты отсутствует. Данный нюанс очевидно и был учтен при проверке всего SecuROM HWID. Рекомендуется воспользоваться этой опцией, если Вы уверены, что активация слетает из-за некорректных значений HWID. После её применения обновите свой HWID путём нажатия кнопки «MY HWID» в главном окне.

* WORD или 2 bytes

Детальная раскладка активного HWID отображается в окне [80_PA]SecuROM HWID (данные можно только смотреть, изменения в этом окне не сохраняются). Правильно сгенерированный unlock code будет привязан только к Вашему компьютеру и никто другой не сможет воспользоваться им (за исключением эмуляции значений HWID, используя, например, хуки WinAPI)

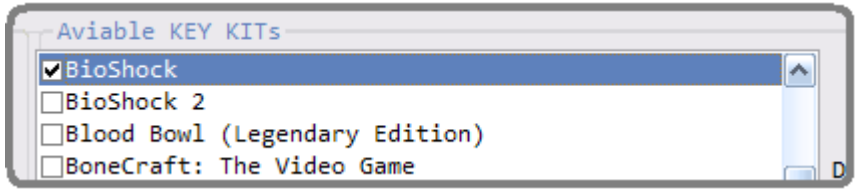


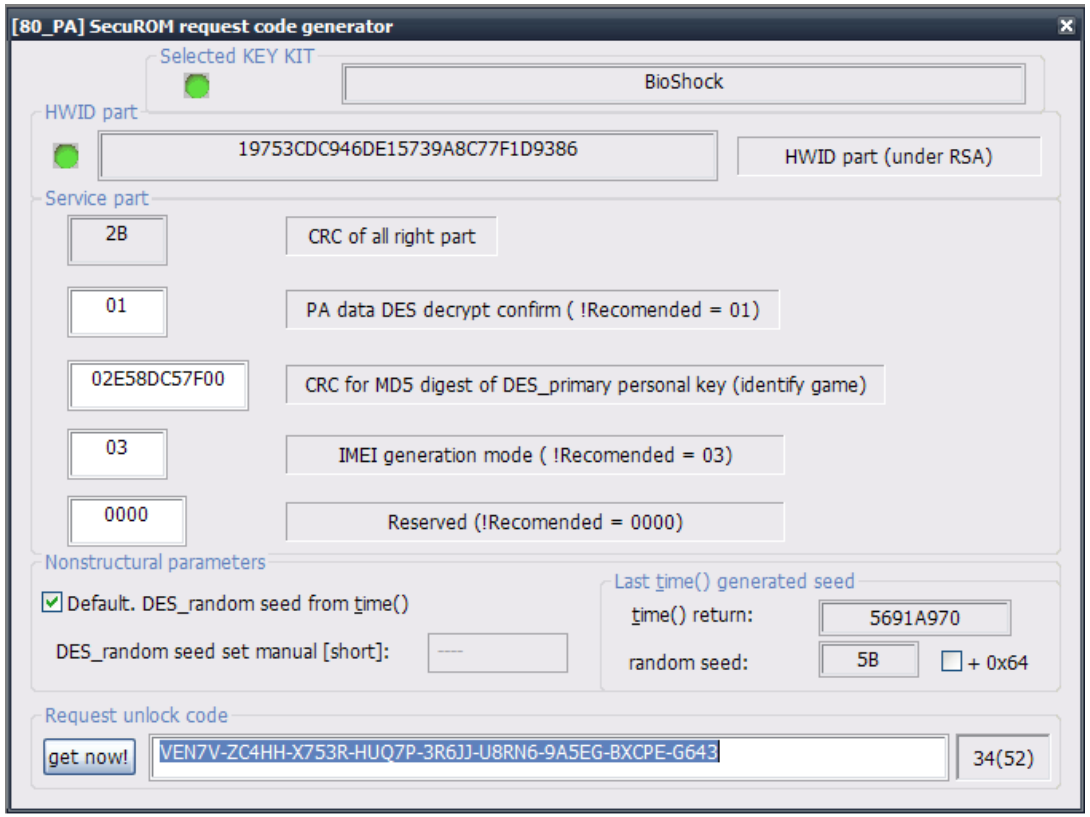
Быстрая расшифровка любых unlock code осуществляется в окне [80_PA] SecuROM Unlock Code Decoder



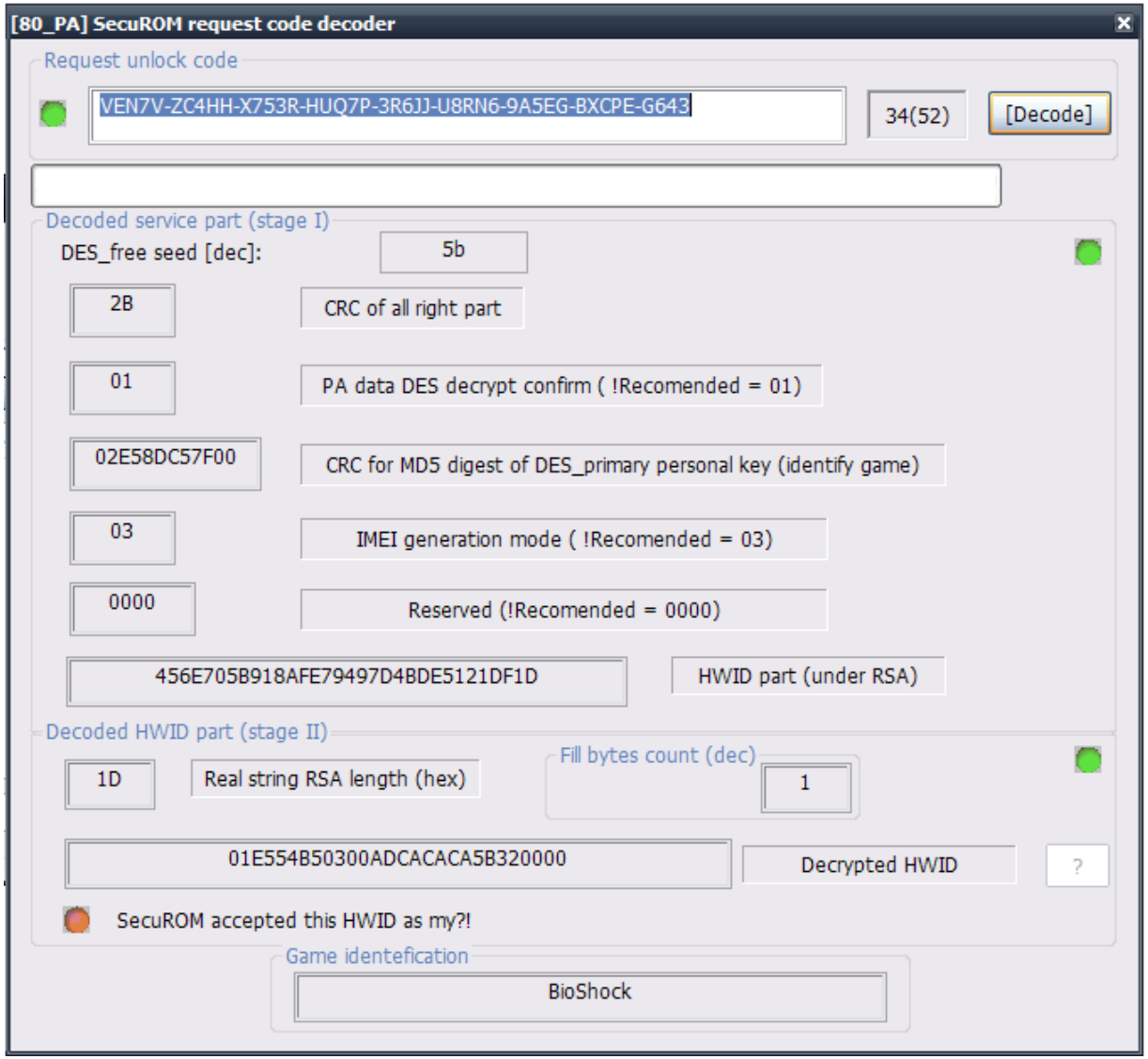
80_PA RUS

Чтобы воспользоваться генератором unlock requestcode (кодом-запросом) [80_PA] SecuROM request code generator необходимо предварительно выбрать игру в главном окне.

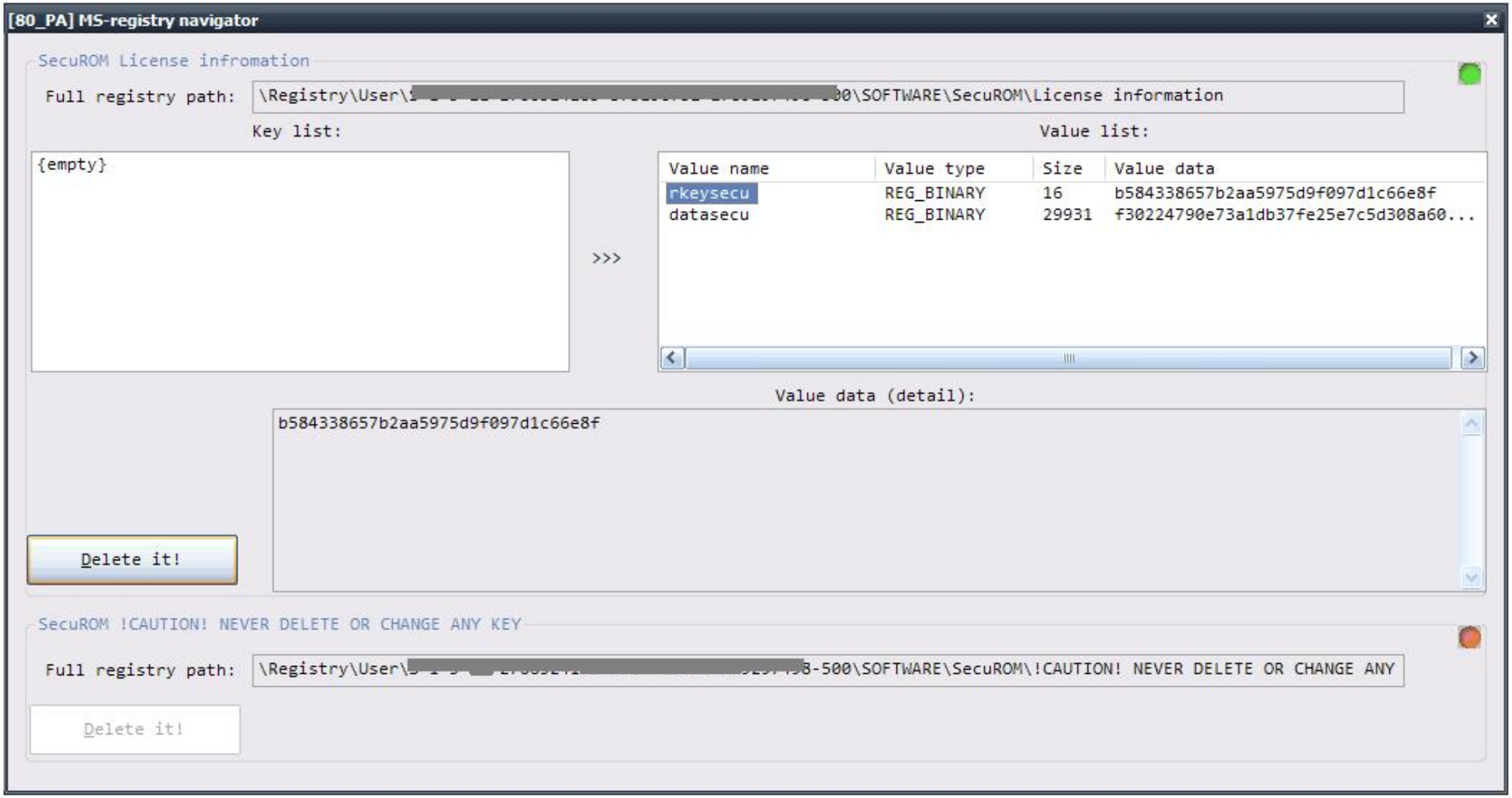




Декодировать любой unlock request code (как это делает сервер активации Sony DADC AG) можно в окне [80_PA] SecuROM request code decoder.

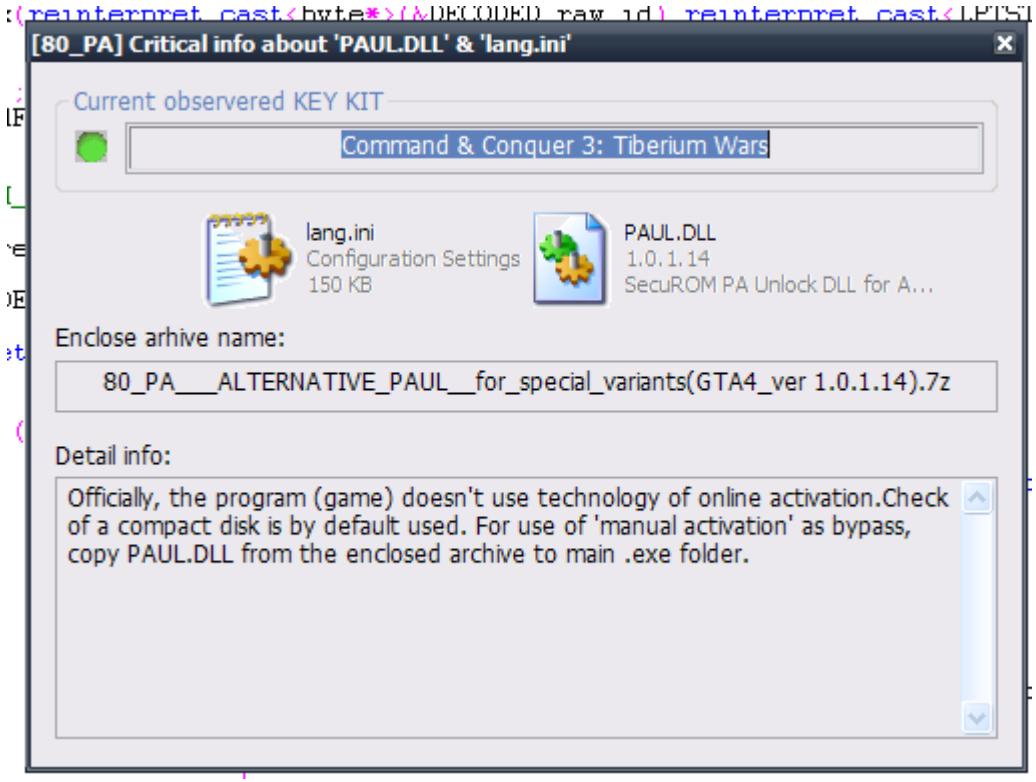


Вытаскивание данных из скрытого ключа License information, а также его удаление вместе с !CAUTION! NEVER DELETE OR CHANGE ANY KEY осуществляется в окне [80_PA] MS-registry navigator.

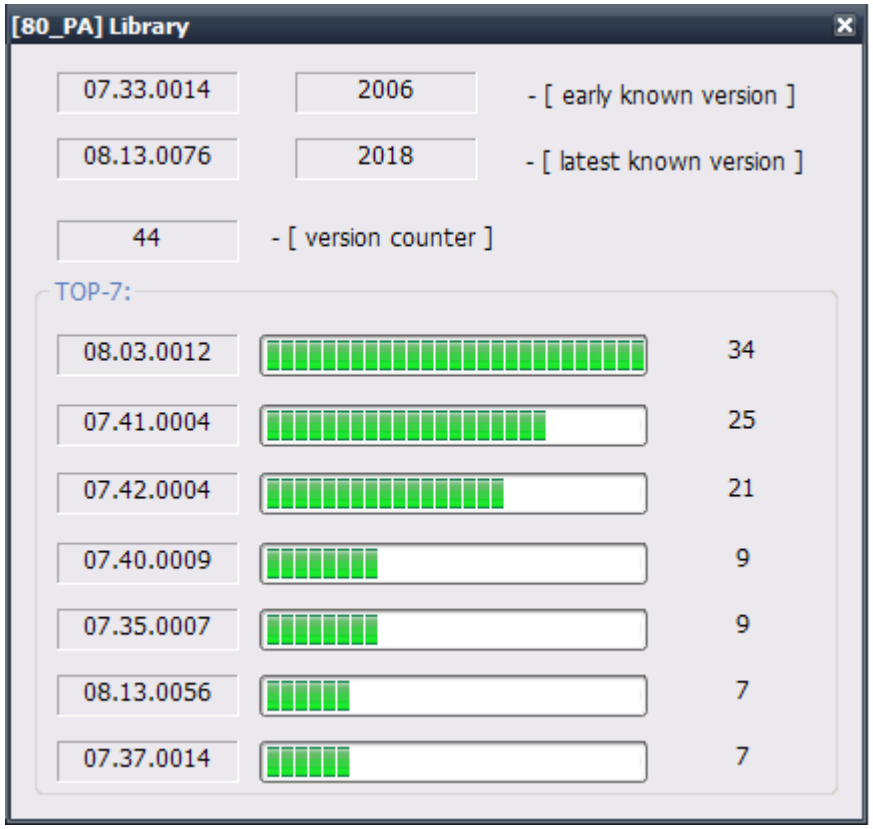


Окно [80_PA] Critical info about 'PAUL.DLL' & 'lang.ini' непосредственно связано с пиктограммами 

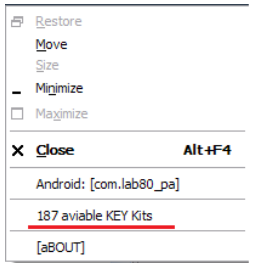
, которые отображаются в главном окне. Собственно окно содержит картинку с файлами «lang.ini» и «paul.dll», а также информирует о рекомендуемом прилагаемом архиве из папки *«80_PA addons»* (если в Вашем случае наблюдаются проблемы, попробуйте подобрать архив с другими версиями библиотеки-обвертки «paul.dll»), из которого необходимо достать оговариваемые файлы для взвода «Manual Activation». Также может указываться важная дополнительная информация, необходимая для корректного завершения процедуры активации.



В более поздних версиях ver.2.0 появилась статистика из библиотеки [80_PA] Library по известным версиям Sony DADC AG SecuROM.

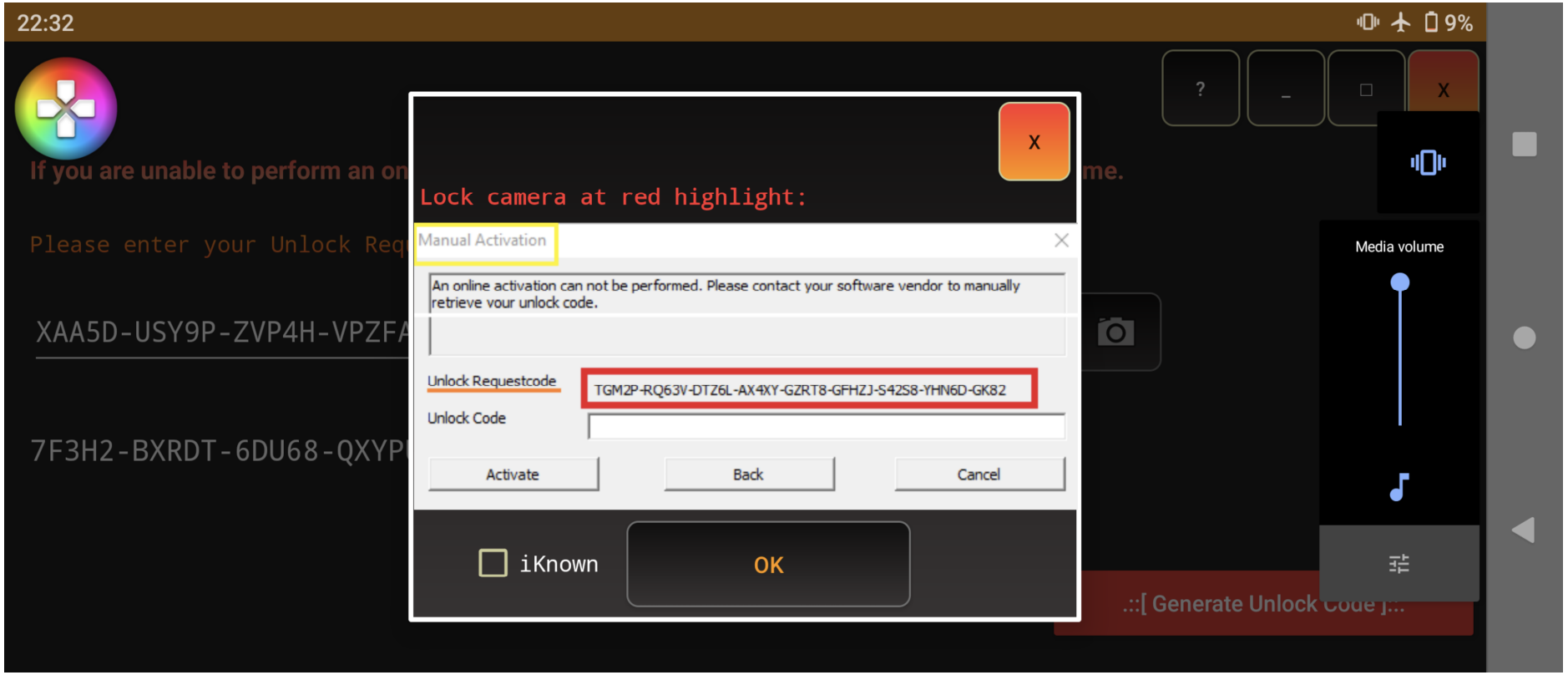


Доступно через главное меню 80_PA SecuROM keygen:



Android версия: com.lab 80pa

Написана гораздо позже, часть кода кейгена была переработана для корректной компиляции в LLVM. Далее изменения были перенесены в версию v.2.0 на Windows (Intel C/C++). Принципиально ничем не отличается от v.2.0 за исключением метода ввода «Request Unlock Code» – через камеру смартфона путём распознания текста (прицел 1Г46).



https://www.amazon.com/gp/product/B0DQZWXQQ8

https://www.rustore.ru/catalog/app/com.lab80_pa

Android 4.0+ (Ice Cream Sandwich, API 14) или выше

MacOSX «Cider» / Linux Wine

Cider - приложение в Mac OS X, которое запускает в этой среде Windows игры, накрытые SecuROM 7-8. Поведение 80_PA, в данном случае, АНАЛОГИЧНО Windows среде, в которой берётся Ваш персональный HWID и генерируется unlock code. Тем не менее, в случае возникающих проблем с генерацией unlock code или запуска 80_PA в среде Linux/Mac OS X через эмуляторы Wine/Cider (на данный момент не зафиксировано нативных игр/программ для Linux/Mac OS X, которые использовали когда либо SecuROM DRM), проще всего запустить 80_PA SecuROM keygen на обычном компьютере с установленной Windows XP-11 и сгенерировать ответный unlock code по известному request unlock code, который указан в окне активации вручную (manual activation).

Для ранних версий 80_PA в среде Linux требовалась дополнительная установка mfc42.dll:

```
sudo add-apt-repository ppa:ubuntu-wine/ppa
sudo apt-get update && sudo apt-get upgrade
winetricks mfc42
```

В более поздних версиях такая опция более не требуется.



Раскрытие исходного кода генерации HWID и структур unlock (request)code.

```
#include "80_PA.h"
/*
                                                ELF present:

       ---------      ---------              ------------         -----------
      ----     ----  ----   ----             ----      ----      ----     ----
      ----     ----  ----   ----             ----      ----     ----       ----
      ----     ----  ----   ----             ----      ----     ----       ----
       ----------   ----   ----             ------------      ----       ----
      ----     ----  ----   ----             ----                -----------
      ----     ----  ----   ----             ----               ----       ----
      ----     ----  ----   ----             ----               ----       ----
        ---------     ---------   ----------- ----              ----       ----
                  Russian Hackers SecuROM PA (online-activation) project
                                                    EXELAB.RU
*/
// LOCK идентификация
#define PA_UNLOCK_CODE_lock__NO_LOCK 0 //НЕТ БЛОКИРОВКИ
#define PA_UNLOCK_CODE_lock__LOCK_ENDDATE 4 //БЛОКИРОВКА ПО КОНЕЧНОЙ ДАТЕ ПОЛЬЗОВАНИЯ
#define PA_UNLOCK_CODE_lock__LOCK_NUMBERDAYS 3 //БЛОКИРОВКА ПО ДНЯМ
#define PA_UNLOCK_CODE_lock__LOCK_NUMBERLAUNCHES 2 //БЛОКИРОВКА ПО КОЛИЧЕСТВУ ЗАПУСКОВ
#define PA_UNLOCK_CODE_lock__LOCK_PLAYTIME 1 //БЛОКИРОВКА ПО ВРЕМЕНИ В ИГРЕ




// структура SecuROM unlock code //
80_PA RUS
```

```
#pragma pack(1)
typedef      struct sc_lock_part //LOCK - опции блокировки ключа
             {
             unsigned short T80_LOCK_INT_DATA; // данные блокировки (2 байта)

             byte T80_LOCK_TYPE_IDENT; //идентификатор типа блокировки (1 байт)
             }lock_part;

typedef      struct sc_imei_part //зашифрованный HWID
      {
             byte T80_IMEI[15]; //зашифрованное значение HWID(15 байт)
             byte T80_IMEI_as_RSA_string_Length; //длина шифрованного значения HWID в строчном ASCII-формате (1 байт)
      }imei_part;

 typedef struct ELF_80_PA_UNLOCK_CODE
{
byte T80_CRC_of_right_part; //CRC правой части (1 байт)
byte T80_Activate_count; //Контрольный байт активации (1 байт)
unsigned short T80_CRC_of_MD5_Serial_num; //Дайджест серийного номера (2 байта)
byte T80_CRC_of_MD5_DES_PRIMARY_key_digest[2]; // Дайджест от appid ( 2 байта)

lock_part lock;
imei_part imei;

}T_80_unlock;

//структура unlock requestcode //
typedef struct ELF_80_PA_REQUEST_UNLOCK_CODE
{
byte T80_PA_CRC_Polynom; // CRC правой части (1 байт);
byte T80_PA_DES_Success_decrypt_confirm; //DES success (1 байт)
byte T80_PA_CRC_MD5_digest_of_DES_prep[6]; // Дайджест от appid (6 байт)
byte T80_PA_REQUEST_MODE_generation; //режим генерации (1 байт)
byte T80_PA_reserved_unkwnown[2]; //неизвестно. [возможно переходящие LOCK BYTE] (2 байта)
imei_part imei;
```

80_PA RUS

```
}T_80_request_unlock, *pT_80_request_unlock;

// структура SecuROM HWID //
typedef struct RAW_MACHINE_ID
{
	bool IsRealTimeGenerated;
	byte Version_nfo_hashik;
	WORD System_nfo_hashik;
	byte VideoBoard_nfo_hashik;
	byte Reserved1;
	byte Network_nfo_hashik;
	WORD Reserved2;
	byte Reserved21;
	WORD System_HardDisk_serial_nfo_hashik;
	WORD Secondary_HardDisks_serial_nfo_hashik;
	byte Null_terminant;
}pa_raw_hwid, *ppa_raw_hwid;
#pragma pack()

// Маска проверки объектов HWID //
typedef struct VERIFY_MASK_HWID
{
	bool Verify_IsRTG_flag;
	bool Verify_Version_nfo;
	bool Verify_System_nfo;
	bool Verify_VideoBoard_nfo;
	bool Verify_Reserved1;
	bool Verify_Network_nfo;
	bool Verify_Reserved2;
	bool Verify_HardDisk_serial_nfo;
	bool Verify_HardDisk_secondary;
}PA_verify_mask_hwid;
PA_verify_mask_hwid pa_current_config = {1,1,1,0,0,0,1,0}; // Дефолтное состояние проверки HWID, зашитое в SecuROM
// Процедура сборки SecuROM HWID //
void Get_raw_machine_ID(ppa_raw_hwid raw_ID)
{
```

```
/* 1 step */
OSVERSIONINFO osinfo;
SYSTEM_INFO sysinfo;
D3DADAPTER_IDENTIFIER9 gpu_info;

PIP_ADAPTER_INFO pAdapterInfo;
ULONG ulOutBufLen = (sizeof (IP_ADAPTER_INFO )*8);



unsigned long MD5_Data[32]; //128 (0x80) bytes !!!

memset((void*)raw_ID,0,sizeof(RAW_MACHINE_ID));

raw_ID->IsRealTimeGenerated=true;

 /* 1 step */ //(информация об ОСи)
memset(&osinfo,0,sizeof(OSVERSIONINFO));
memset(&MD5_Data[0],0,sizeof(MD5_Data));
MD5_CTX md5context;

osinfo.dwOSVersionInfoSize = sizeof(OSVERSIONINFOEX);
::GetVersionEx(&osinfo);


                    MD5_Init(&md5context);


                    md5context.Nl = MD5_Cont_Size;
                    md5context.Nh = 0;
                    md5context.num=MD5_DIGEST_LENGTH;
                    md5context.data[0] = osinfo.dwMajorVersion;
                    md5context.data[1] = osinfo.dwMinorVersion;
                    md5context.data[2] = osinfo.dwBuildNumber;
                    md5context.data[3] = osinfo.dwPlatformId;

                    MD5_Final((unsigned char*)&MD5_Data[0], &md5context);


               QUCK_XOR_RAW_DATA(&raw_ID->Version_nfo_hashik,(byte*)&MD5_Data[0],sizeof(test_raw_hwid.Version_nfo_hashik));
```

```
	/* 2 step */ //(информация об установленном процессоре)
	::GetSystemInfo(&sysinfo);

			MD5_Init(&md5context);

			md5context.Nl = MD5_Cont_Size;
			//md5context.Nh = 0;
			md5context.num=MD5_DIGEST_LENGTH;
			md5context.data[0]=sysinfo.dwProcessorType;
			md5context.data[1]=sysinfo.dwAllocationGranularity;
			md5context.data[2]=sysinfo.wProcessorLevel;
			md5context.data[3]=sysinfo.wProcessorRevision;

			MD5_Final((unsigned char*)&MD5_Data[0], &md5context);

		QUCK_XOR_RAW_DATA((byte*)&raw_ID->System_nfo_hashik,(byte*)&MD5_Data[0],sizeof(test_raw_hwid.System_nfo_hashik));

	/* 3 step */ //(информация об установленной видеокарте)
	HMODULE h_lib = LoadLibrary("d3d9.dll");

		if (h_lib != NULL)
		{
		D3D9Create=(d3d9_create)GetProcAddress((HMODULE)h_lib,"Direct3DCreate9");

		PDIRECT3D9 d3d9struct = D3D9Create(D3D_SDK_VERSION);

		d3d9struct->TABLE_d3d9->GetAdapterIdentifier(d3d9struct, D3DADAPTER_DEFAULT,D3DENUM_WHQL_LEVEL, &gpu_info);

		FreeLibrary(h_lib);

			MD5_Init(&md5context);

			md5context.Nl = MD5_Cont_Size;
			//md5context.Nh = 0;
			md5context.num=MD5_DIGEST_LENGTH;
			md5context.data[0]=gpu_info.VendorId;
			md5context.data[1]=gpu_info.DeviceId;
			md5context.data[2]=gpu_info.SubSysId;
			md5context.data[3]=gpu_info.Revision;

			MD5_Final((unsigned char*)&MD5_Data[0], &md5context);
```

```
	QUCK_XOR_RAW_DATA(&raw_ID->VideoBoard_nfo_hashik,(byte*)&MD5_Data[0],sizeof(test_raw_hwid.VideoBoard_nfo_hashik));

	}

/* 4 step */ //(информация о сетевой карте) offline/online mode
h_lib = LoadLibrary("IPHLPAPI.dll");
	if (h_lib != NULL)
	{

		 pAdapterInfo = (IP_ADAPTER_INFO *) malloc(sizeof (IP_ADAPTER_INFO)*8);
		IPGetAdaptersInfo=(IPHLPAPI_GetAdaptersInfo)GetProcAddress((HMODULE)h_lib,"GetAdaptersInfo");



	IPGetAdaptersInfo(pAdapterInfo, &ulOutBufLen);

		FreeLibrary(h_lib);

		MD5_Init(&md5context);

		md5context.data[1]=0;
		memcpy(&md5context.data[0],pAdapterInfo->Address,sizeof(pAdapterInfo->Address));
		md5context.Nl = MD5_Cont_Size_for_IPHLAPI;
		md5context.num=MD5_DIGEST_LENGTH-10;


		md5context.data[2]=0;
		md5context.data[3]=0;


			MD5_Final((unsigned char*)&MD5_Data[0], &md5context);

		QUCK_XOR_RAW_DATA(&raw_ID->Network_nfo_hashik,(byte*)&MD5_Data[0],sizeof(test_raw_hwid.Network_nfo_hashik));

	free((void*)pAdapterInfo);
	}
/* 5 step*/ //в оригинале там цикл опроса через GetDriveType(c:..z:) с первым попавшимся HDD (читай ищется системный HDD)
		char NameBuffer[MAX_PATH];
		char SysNameBuffer[MAX_PATH];
```

```
		DWORD VSNumber=0;
		DWORD MCLength=0;
		DWORD FileSF=0;
		char disk[3];
		disk[1]=*":";
		disk[2]=*"\\";
		disk[3]=0x0u;


	for( disk[0] = *"c"; disk[0] <= *"z";disk[0]=(byte)disk[0]+1)
	{


		if (::GetDriveType(&disk[0]) == DRIVE_FIXED)
		{
::GetVolumeInformation(&disk[0],NameBuffer, sizeof(NameBuffer), &VSNumber,&MCLength,&FileSF,SysNameBuffer,sizeof(SysNameBuffer));
			break;
		}

	}
	__asm //SWAP VSNumber
	{
		MOV EAX, DWORD PTR SS:[VSNumber]
		BSWAP EAX
		MOV DWORD PTR SS:[VSNumber], EAX
	}

		MD5_Init(&md5context);

		md5context.Nl = (MD5_Cont_Size/4);
		md5context.num=(MD5_DIGEST_LENGTH/4);
		md5context.data[0]=VSNumber;
		md5context.data[1]=0;
		md5context.data[2]=0;
		md5context.data[3]=0;


		MD5_Final((unsigned char*)&MD5_Data[0], &md5context);

QUCK_XOR_RAW_DATA((byte*)&raw_ID-
>System_HardDisk_serial_nfo_hashik,(byte*)&MD5_Data[0],sizeof(test_raw_hwid.System_HardDisk_serial_nfo_hashik));
```

8O_PA RUS

```
                raw_ID->Null_terminant=NULL;

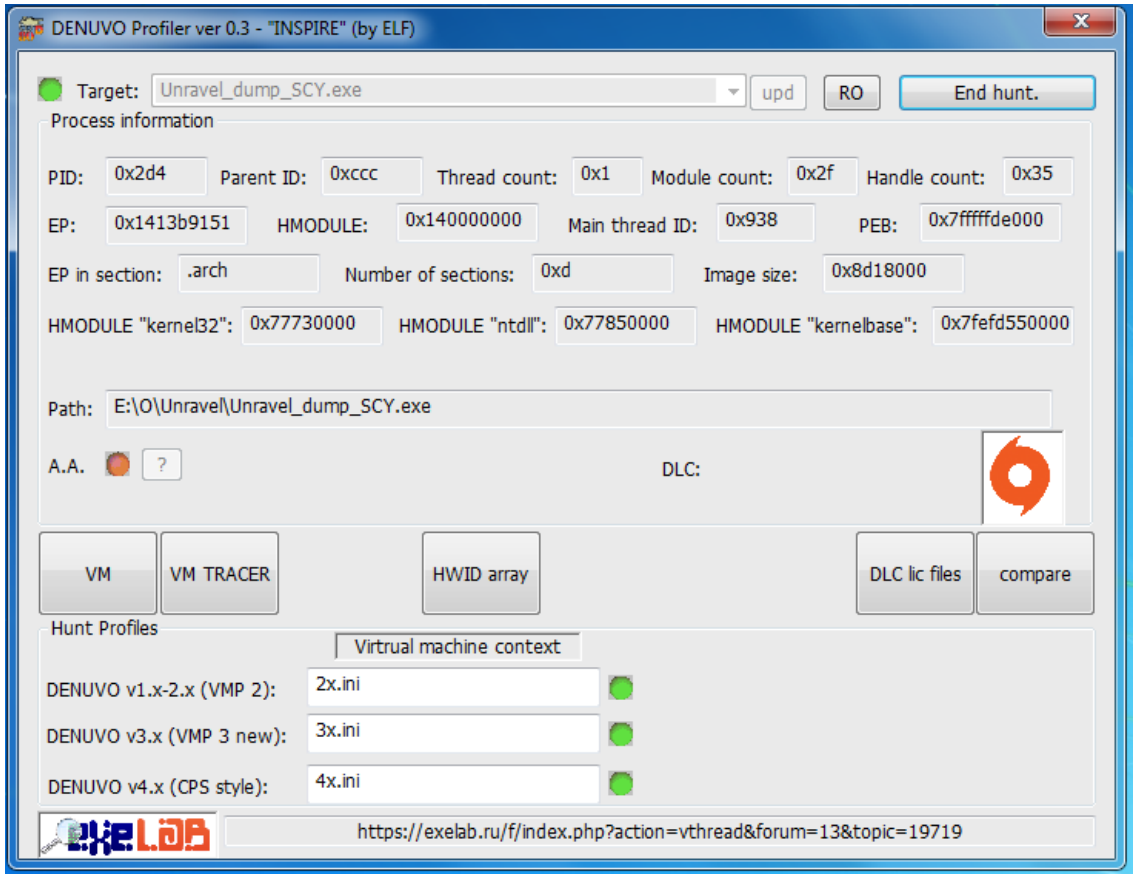

}

// вспомогательная функция шифрования данных в HWID
void __inline __fastcall QUCK_XOR_RAW_DATA (byte* Desdonation, byte* MD5_CTX_start, DWORD Xoring_size)
{
	for(unsigned long i=1; i<=(sizeof(MD5_LONG)*4); i++)
	{
		for(unsigned long k=0; k<=Xoring_size-1; k++)
		{
			*(Desdonation+k) ^= *(MD5_CTX_start++);
		}

	}
}
```

Другие проекты.

На самом деле их больше



DENUVO_Profiler (DProfiler) – **«be preparing to dominate to one of famous DRM on the world»**



diff_trace – программа для сравнения двух trace-логов (трассировка), сохраненных отладчиком OllyDbg 2.x (или его аналогами). *diff_trace* был использован для взлома модуля проверки геометрии дисков SecuROM. Распространяется с исходными текстами. (https://exelab.ru/f/index.php?action=vthread&forum=3&topic=20942)


T80 SPR I (SecuROM Profiler) – программа-помощник для работы с виртуальными машинами (virtual machine) SecuROM v7.3x – v8.x. Включает в себя контроль anti-attach (A.A.) для присоединения к уже запущенному защищенному процессу. (https://exelab.ru/F/index.php?action=vthread&forum=13&topic=19719)


DUNE 2009 (DUNE_LAUNCH.exe) – оригинальная игра DUNE 2000 от **WestWood Studios** с измененным движком. (http://rutracker.org/forum/viewtopic.php?t=3637042)



Dark Colony – оригинальная вылеченная игра Dark Colony (Alcohol 120% для монтирования образа не требуется вообще!). Исправлены некоторые ошибки и баги. Добавлены программы **DC_SAV**(редактор сохранений) и **DC_RET**(для корректного возвращения в игру при переключении **Alt+Tab**) (http://rutracker.org/forum/viewtopic.php?t=3683906)


DOoM 2 game – несерьезная простенькая игрушка, написанная в 2006г. назад на VB 6 на тему уничтожения "Дом-2". (http://rutracker.org/forum/viewtopic.php?t=3703290)



HEIDENHAIN TNCremoNT (Plus) + TeleService – взломанные версии известных программ для обмена данными со станками ЧПУ TNCremoNT и TeleService.(https://rutracker.org/forum/viewtopic.php?t=5426612)

Atlassasin Jira & Confluence private crack – самые крайние версии + плагины из Marketplace. По заказу.

CIMCO Software – CIMCO A/S. CIMCO Edit 2025, 8, 6 + перекидывание файлов. **CTranslate** (CIMCO Translate) – утилита для чтения/редактирования language (языковых) файлов CIMCO, добавление собственного перевода программных продуктов CIMCO.

Google Chrome 141 for Windows 7 (с поддержкой WebGPU)

https://habr.com/ru/articles/752692/

https://habr.com/ru/articles/789120/

https://github.com/Blaukovitch/GOOGLE_CHROME_Windows_7_CRACK

https://rutracker.org/forum/viewtopic.php?t=6384596

О проекте 80 PA. Обратная связь.

Автор технологии 80_PA, взлом SecuROM: **ELF**

Выражаем огромную благодарность: random (manager of key kits)

Archer (solutions explorer),

 int (PA unlock page)

reversecode (алгоритм DES)

Nightshade (advices)

mak (old SecuROM info)

Haoose (www.antistarforce.com)

painter *(v00doo)*

mysterio

gig3x , HardcoreHacker[HcH], Tihamér Szabó

Спасибо всем остальным участникам за поддержку:

OnLyOnE, ARCHANGEL, Bronco, Vovan666, VodoleY, DimitarSerg, DenCoder, Gideon Vi, MasterSoft, BAHEK, ClockMan, SReg, [Nomad], daFix, 4kusNick, Ara, Smon, DillerInc, Dart Raiden, zeppe1in, kioresk, SER[G]ANT, DeZoMoR4iN, ajax, vovanre, SharkXXL, too87264 *и всем остальным, кого не перечислил!*

Отдельное благородное спасибо: Sony DADC AG (*теперь уже* «Denuvo Software Solution GmbH») ☺

https://exelab.ru/f/PAunlock/

https://exelab.ru/f/index.php?action=vthread&forum=13&topic=19719

http://exelab.ru/rar/dl/CRACKLAB.rU_107.rar

https://youtu.be/AcVTF1HfTb8
https://youtu.be/x6M5bOvv0Fg

http://rutracker.org/forum/viewtopic.php?t=5116975

http://antistarforce.com/forum/8-16870-1

https://xakep.ru/2015/08/07/securom/
https://xakep.ru/2019/04/19/denuvo/

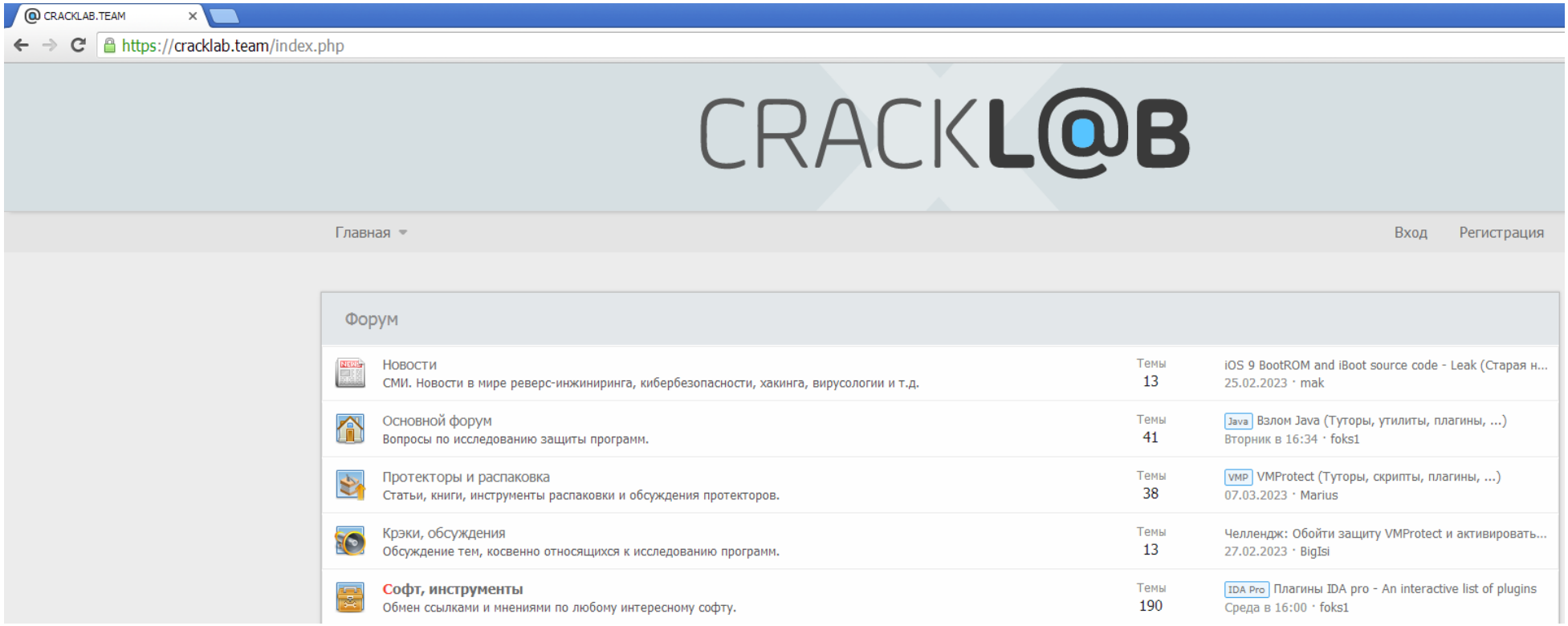
https://tuts4you.com/download.php?view.2090

https://cracklab.team/PAunlock/

https://github.com/Blaukovitch/80_PA/releases

https://www.reddit.com/r/Piracy/comments/42nt1h/what_is_this_crack_securom_denuvo/

securom80pa(at)gmail.com



- **Новости взлома**
- **Протекторы и их распаковка**
- **Обсуждение Ваших проектов**
- **Популярные хакерские инструменты и утилиты**
- **Вопросы-ответы по взлому**
- **Техническая документация**
- **Электроника и криптография**

UNLOCK CODE	Game
KF3HC-7UZJ9-U3BDV-MP4QD-8B...	Epic Mickey 2: The Power of Two
KF3HC-7UXKY-CSL8G-N4SSK-RM...	Grand Theft Auto IV
CH746-RKFD5-KCZTP-8FLP4-2J...	Epic Mickey 2: The Power of Two
CH746-RKHM3-TTK5V-ZLN8A-27...	Grand Theft Auto IV

«Тибериумный реверсинг»

(C) 2011-2026. ELF

