

# Установка отладчика SoftICE на Windows XP SP1, SP2

Автор: Bad\_guy <[bad\\_guy@cracklab.ru](mailto:bad_guy@cracklab.ru)> [www.CRACKLAB.ru](http://www.CRACKLAB.ru)

В настоящее время стала популярной операционная система Windows XP, ну а Windows 98 отошла на задний план. Вместе с этим возникла проблема для начинающих крэкеров с установкой отладчика SoftICE. В данной статье попробую предложить несколько решений данной проблемы, так как на основе анализа форума я понял, что это "больной" вопрос, который заданный кем-то снова всегда висит на первой странице форума и раздражает аборигенов.

Разберём три варианта установки отладчика SoftICE под WinXP SP2. Замечу сразу, что от версии Windows XP - Service Pack 1 или Service Pack 2 практически ничего не зависит в данном случае и, так как, у меня всё же Service Pack 2, то в любом случае должна быть "обратная совместимость" с Service Pack 1.

## ВАРИАНТ 1: Установка SoftICE 4.05 WinNT на Windows XP

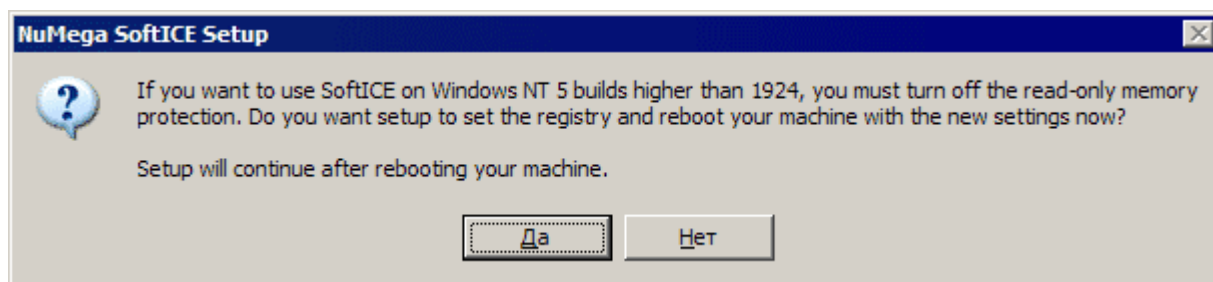
Это старая версия, разработанная для Windows NT, однако, правильно установив его под WinXP можно успешно работать и с этой версией. Преимущество этой версии - размер установочного архива: 5 Мб.

Найти его можно:

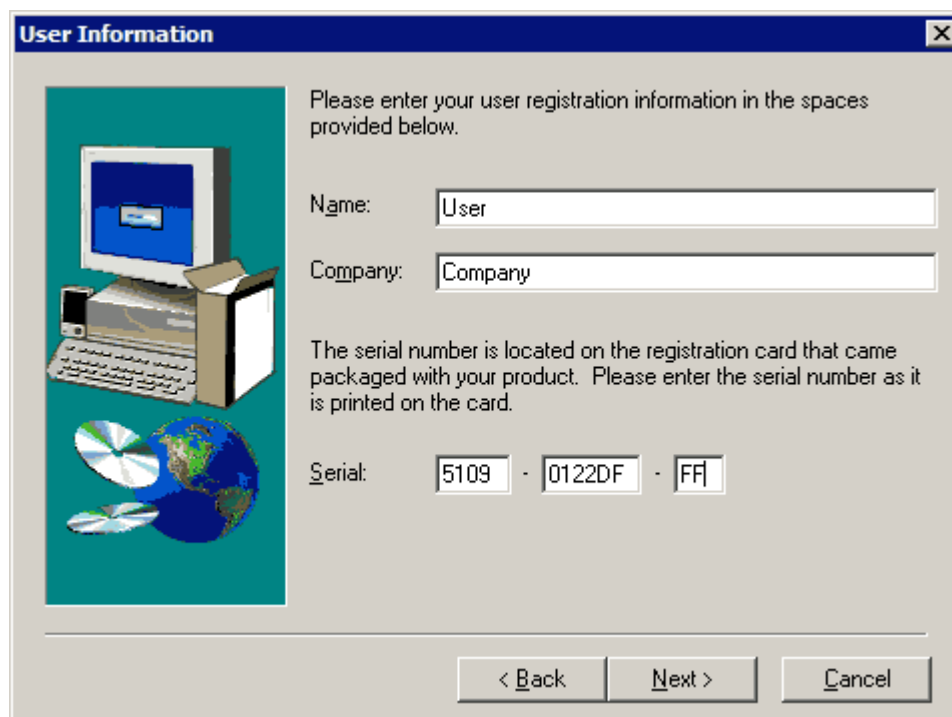
1. <http://cracklab.ru/download/get.php?g=2>
2. <http://reversing.kulichki.net/files/debug/si405wnt.rar>
3. а если эти ссылки накроются, то ищите новую ссылку:  
<http://www.yandex.ru/yandsearch?rpt=rad&text=si405wnt>
4. Также этот дистрибутив я разместил на дисках CRACKL@B CD#1 и CRACKL@B DVD, о которых можно прочитать здесь:  
<http://cracklab.ru/cd.php>

Теперь перейдём к процессу установки, который я специально проделаю прямо сейчас на своём компьютере (хотя уже и пользуюсь SoftICE 4.31), чтобы в данной статье всё было грамотно и "на личном опыте".

Запускаю установку и почти сразу мне выдалось окошко:



Это окно предложило мне, так как у меня Windows XP версия системы выключить защиту памяти "только чтение", естественно, чтобы установить отладчик нужно с этим согласиться, после чего компьютер перезагружается и автоматически запускает продолжение программы установки отладчика, которая мне выдала новое окно, в которое нужно ввести "правильные" данные, примерно вот так:



**User Information**

Please enter your user registration information in the spaces provided below.

Name:

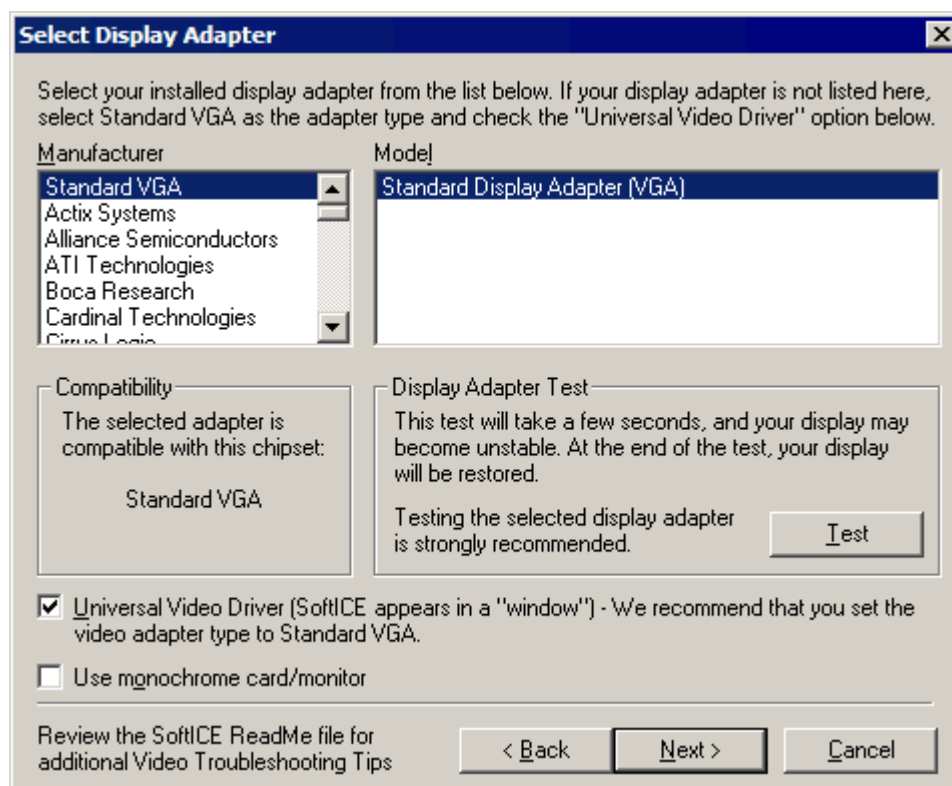
Company:

The serial number is located on the registration card that came packaged with your product. Please enter the serial number as it is printed on the card.

Serial:  -  -

< Back    Next >    Cancel

Далее на экране появится следующее принципиально важное окно, предлагающее выбрать ваш тип видеокарты:



**Select Display Adapter**

Select your installed display adapter from the list below. If your display adapter is not listed here, select Standard VGA as the adapter type and check the "Universal Video Driver" option below.

Manufacturer	Model
Standard VGA	Standard Display Adapter (VGA)
Actix Systems	
Alliance Semiconductors	
ATI Technologies	
Boca Research	
Cardinal Technologies	
Cirrus Logic	

**Compatibility**

The selected adapter is compatible with this chipset:

Standard VGA

**Display Adapter Test**

This test will take a few seconds, and your display may become unstable. At the end of the test, your display will be restored.

Testing the selected display adapter is strongly recommended.

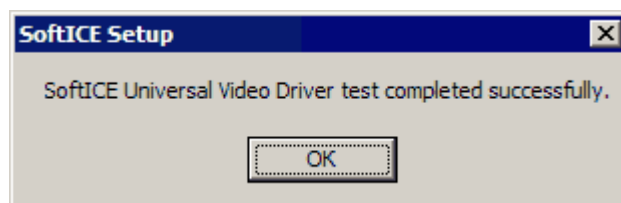
☒ Universal Video Driver (SoftICE appears in a "window") - We recommend that you set the video adapter type to Standard VGA.

☐ Use monochrome card/monitor

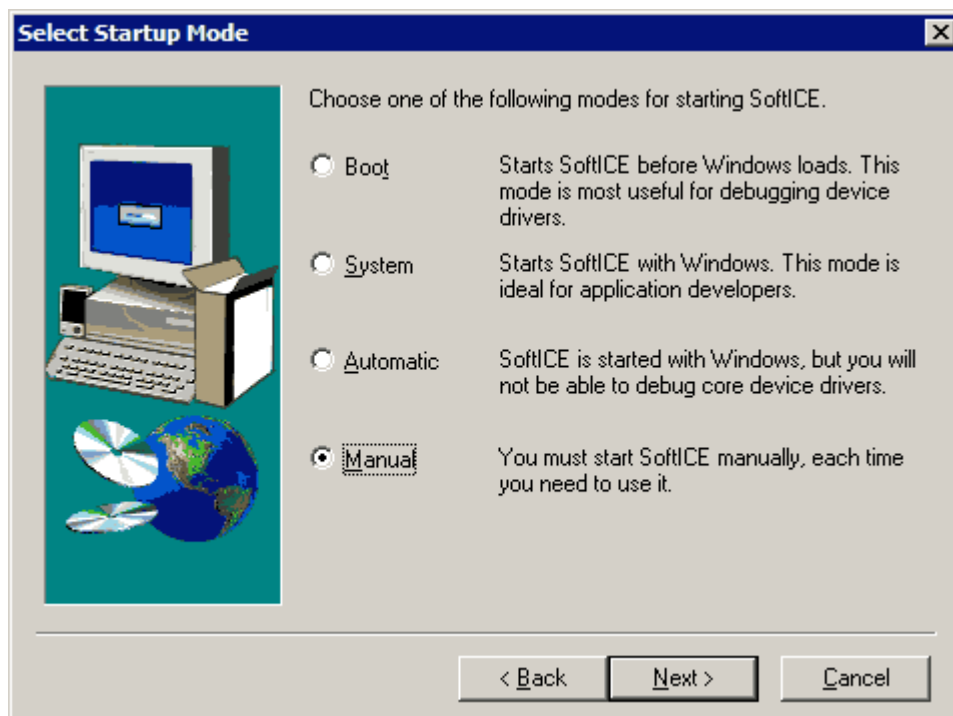
Review the SoftICE ReadMe file for additional Video Troubleshooting Tips

< Back    Next >    Cancel

Но лучше проигнорировать предложение выбрать тип видеокарты и оставить всё именно так как есть и особенно проконтролировать, что галочка "Universal Video Driver" включена, далее нажимаю кнопку "Test" и вижу, что всё в порядке:

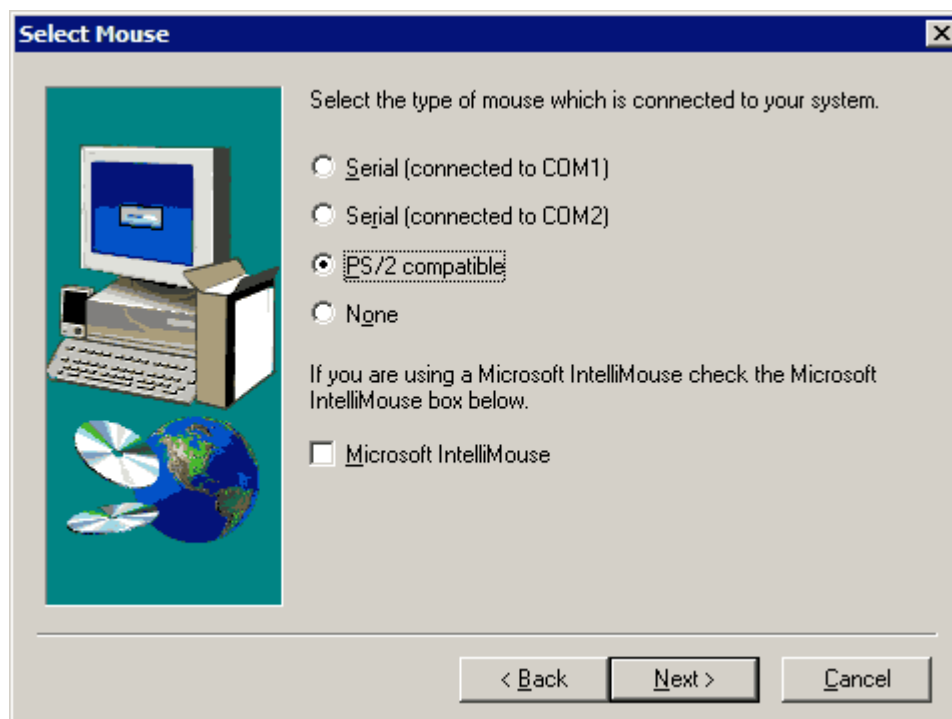


Теперь мы обратим внимание на следующее окно установки отладчика:

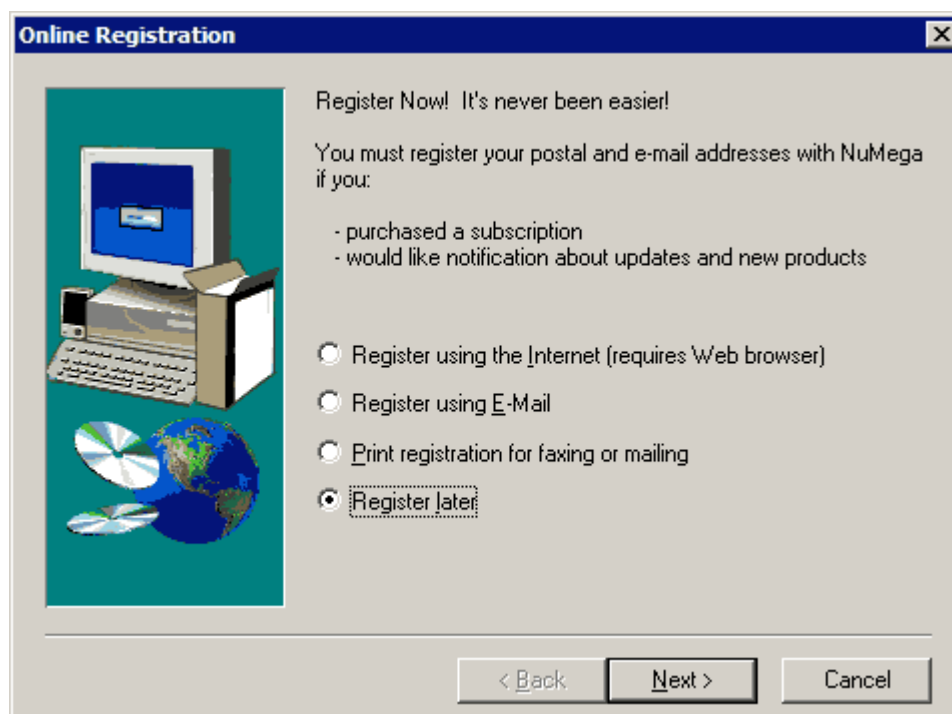


Предлагается выбрать один из четырех вариантов запуска отладчика. По опыту могу сказать, что, на мой взгляд, лучше поставить ручной режим запуска - **Manual**, во-первых, потому, что ежели что случится в процессе установки, то компьютер будет загружаться без проблем, потому как при загрузке софтайс не будет загружаться. Вторая же причина: софтайс "дружит" не со всеми играми и приложениями, поэтому лучше его запускать по необходимости, когда приспичит покрывать чего-нибудь, тем более софтайс после запуска можно выгрузить только одним способом - перезагрузкой. После установки отладчика режим запуска можно будет при желании сменить с ручного на один из терх остальных вариантов, для этого нужно будет пройти в меню "Пуск" - "Все программы" - "NuMega SoftICE" - "Startup Mode Setup".

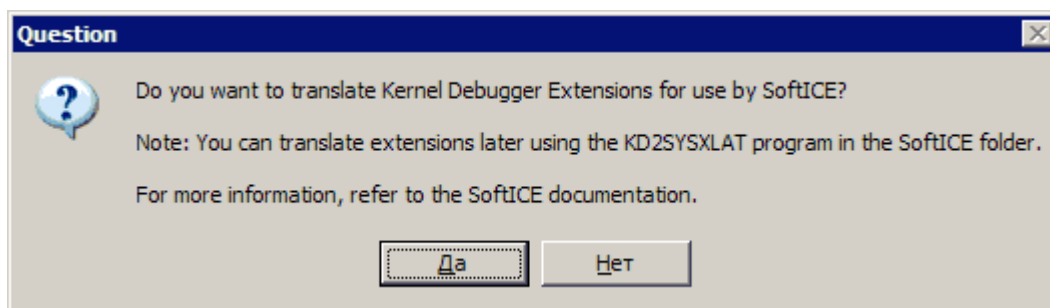
В следующем окне предлагается выбрать порт, к которому подключена мышь. Ответим честно на этот вопрос:



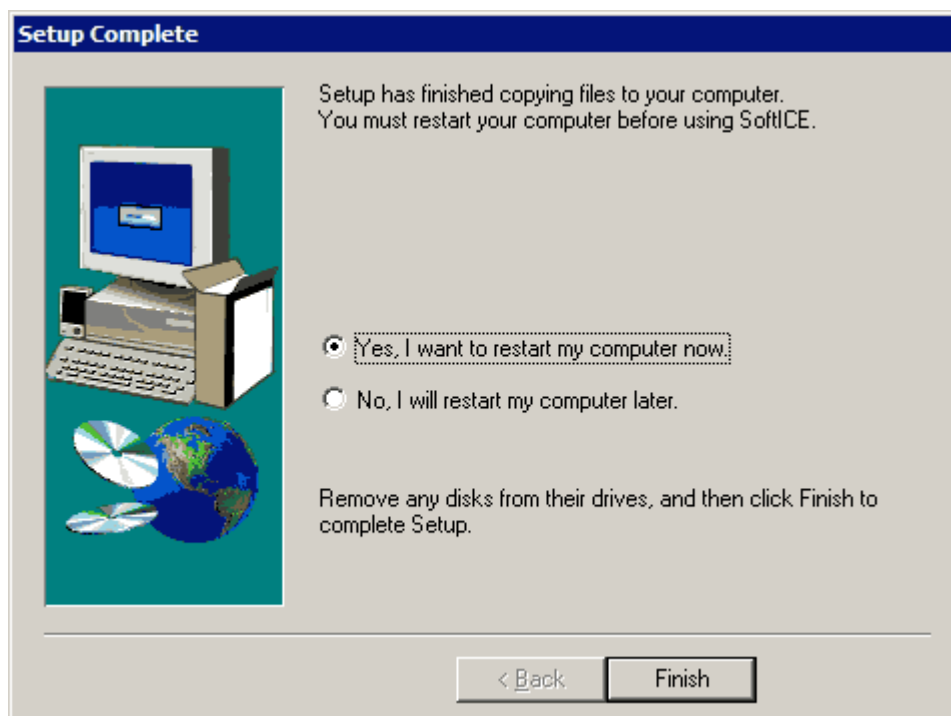
Итак, процесс установки прошёл успешно и высветилось следующее предложение, которое меня лично уже не интересует:



А дальше ещё одно предложение, которое меня "заинтересовало":



Ну и, наконец, давно знакомое и родное каждому юзеру окно:



Перезагружаемся...

После установки в папке `C:\program files\NuMega\SoftIceNT` будет находиться установленный SoftICE, так как мы поставили ручной режим запуска (Manual), то чтобы запустить отладчик нам нужно запустить файл `ntice.bat`, находящийся в той же папке. Файл `ntice.bat` содержит всего лишь одну странную команду: `"net start ntice"`. в этой команде слова `"net start"` - стандартная команда для запуска службы, а вот `"ntice"` - это название службы отладчика SoftICE. Таким образом, после запуска `ntice.bat` должен запуститься отладчик SoftICE, что я сейчас и собираюсь проверить...

Собственно говоря, с запуском отладчика ничего не получилось, так как после запуска `ntice.bat` я нажал комбинацию клавиш `"Ctrl-D"`, которая должна вызывать окно отладчика, если он запущен, но окна отладчика я не увидел. Естественно, решение этой проблемы не придёт "с потолка" и с таким вопросом часто обращаются на форум

<http://cracklab.ru/f/>

Проанализировав архив форума, для чего, кстати, достаточно сходить по ссылке:

<http://cracklab.ru/f/index.php?action=search&searchFor=Softice&eMatch=on&days=1000&searchWhere=1&searchHow=0>

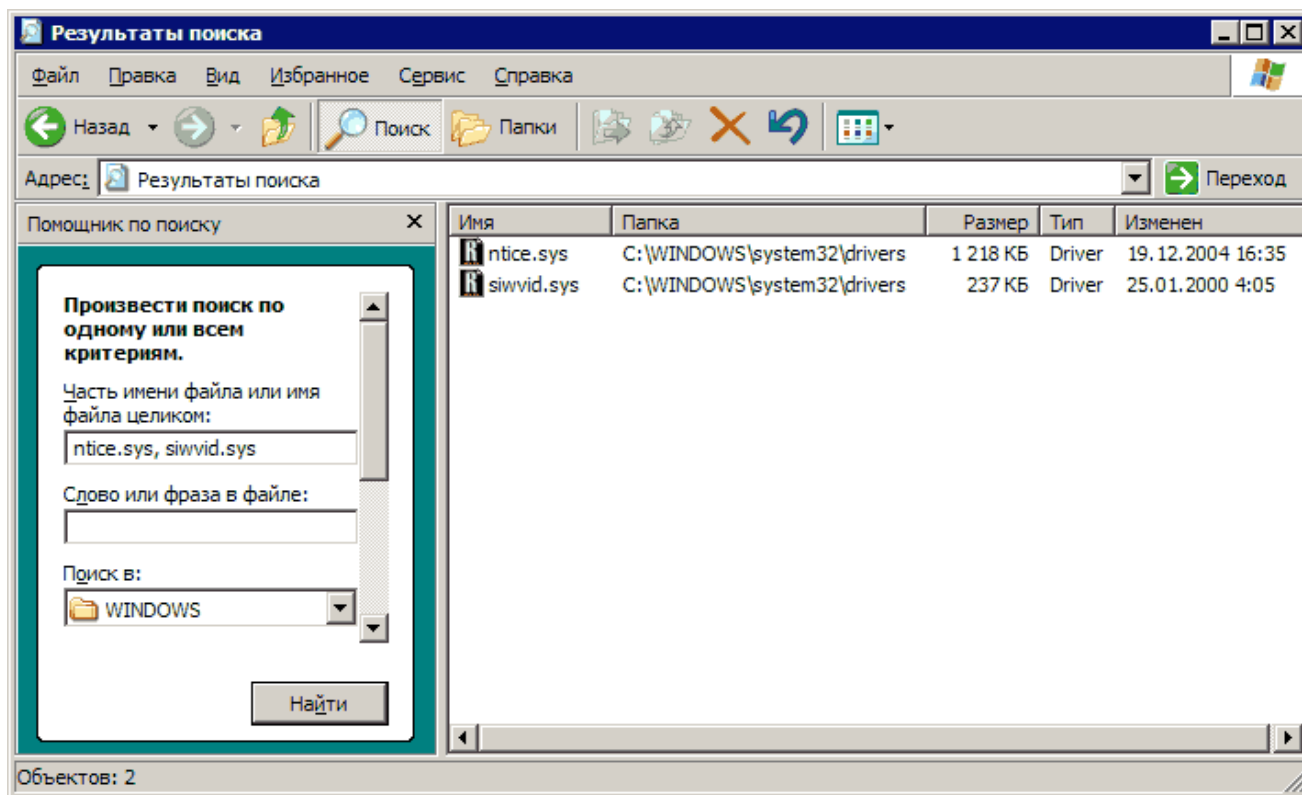
я нашёл несколько топиков, где было написано, что нужно просто скачать дополнительный патч софтайса для WindowsXP, который можно найти:

1. <http://reversing.kulichki.net/files/debug/nticexppatch.rar>
2. <http://cracklab.ru/download/get.php?g=50>
3. <http://www.yandex.ru/yandsearch?rpt=rad&text=nticexppatch>

#### 4. [CRACKL@B DVD](#)

Размер патча: 400 Кб.

В архиве патча находится два файла: `ntice.sys` и `siwvid.sys`, никаких комментариев что делать с этими файлами нет. Но, опять же, по советам с форума становится ясно, что эти файлы надо положить взамен уже существующих файлов где-то в недрах папки `C:\WINDOWS` или той, в которую установлена операционная система. Не будем искать вручную, а воспользуемся встроенным поиском.



Итак, оба файла найдены в папке `C:\WINDOWS\system32\drivers`, теперь нужно заменить их файлами из архива с патчем, что я сейчас и сделаю.

Сразу после замены двух файлов, я снова запустил `ntice.bat` - на этот раз явно было видно, как его окно уже не моментально, а с задержкой исчезло с экрана - этой хороший знак, значит что-то сработало - проверяю, нажав комбинацию "`Ctrl-D`". И экран мне выдаёт сообщение "неоптимальный режим" - рекомендуемый режим `1024*768, 60 Hz`, надо сказать, что у меня LCD-монитор, так что скорее всего дело как раз в этом, но новая проблема "на лицо" - отладчиком по-прежнему нельзя пользоваться, хотя теперь он и запускается. Попытаюсь решить проблему стандартным способом - перезагрузкой, хотя подсознательно понимаю, что скорее всего это в данном случае не поможет...

Надо же, я ошибся - после перезагрузки всё в порядке, во всяком случае теперь запускается окно софтбокса, скриншот которого, к сожалению сделать нельзя, так как софтбокс сидит в нулевом кольце защиты, а "принтскрин" на третьем кольце - в общем, сайс на то и отладчик, чтобы быть "у руля" и не давать собой "рулить" :)

Теперь произведу небольшую настройку айса, для этого найду в той же самой папке `C:\WINDOWS\system32\drivers` файл `Winice.dat`

В нём есть строка

```
INIT="X;"
```

заменим её на

```
INIT="FAULTS OFF; LINES 60; WIDTH 100; WC 40; X;"
```

Эта строка делает вот что: при запуске софтайса первая команда выключает активность софтайса на ошибки системы, три другие команды отвечают за размеры окна софтайса (так окно больше - удобнее получается), последняя команда "X;" - как была, так и осталось в строке - она нужна чтобы при запуске сайса окно его было спрятано. Все эти команды вы можете ввести и вручную вов время аботы отладчика, конечно предварительно вызывав его комбинацией "Ctrl-D".

Теперь в этом же файле Winice.dat нужно удалить все "точки с запятой" около тех строк с названиями файлов, которые действительно есть по этому адресу на вашей машине.

```
; EXP=\SystemRoot\System32\hal.dll  
; EXP=\SystemRoot\System32\ntoskrnl.exe  
; EXP=\SystemRoot\System32\ntdll.dll  
; EXP=\SystemRoot\System32\kernel32.dll  
; EXP=\SystemRoot\System32\user32.dll  
; EXP=\SystemRoot\System32\csrssrv.dll  
; EXP=\SystemRoot\System32\basesrv.dll  
; EXP=\SystemRoot\System32\winsrv.dll
```

После этого сохраните файл, перезагрузите компьютер, запустите снова ntice.bat (ярлык для которого удобно кинуть на рабочий стол).

Возможно, присутствуют какие-то проблемы с работой этого установленного софтайса, но о них тогда позже. Главную задачу - установку можно считать выполненной.

## **ВАРИАНТ 2: Установка SoftICE 4.27 из Compuware DriverStudio 2.7**

Более новая версия отладчика, на этот раз уже не от фирмы Numega, а от Compuware, тоже не порадует нас интуитивно понятным процессом установки :) Однако, размер архива на это раз больше порадует - 3 Мб.

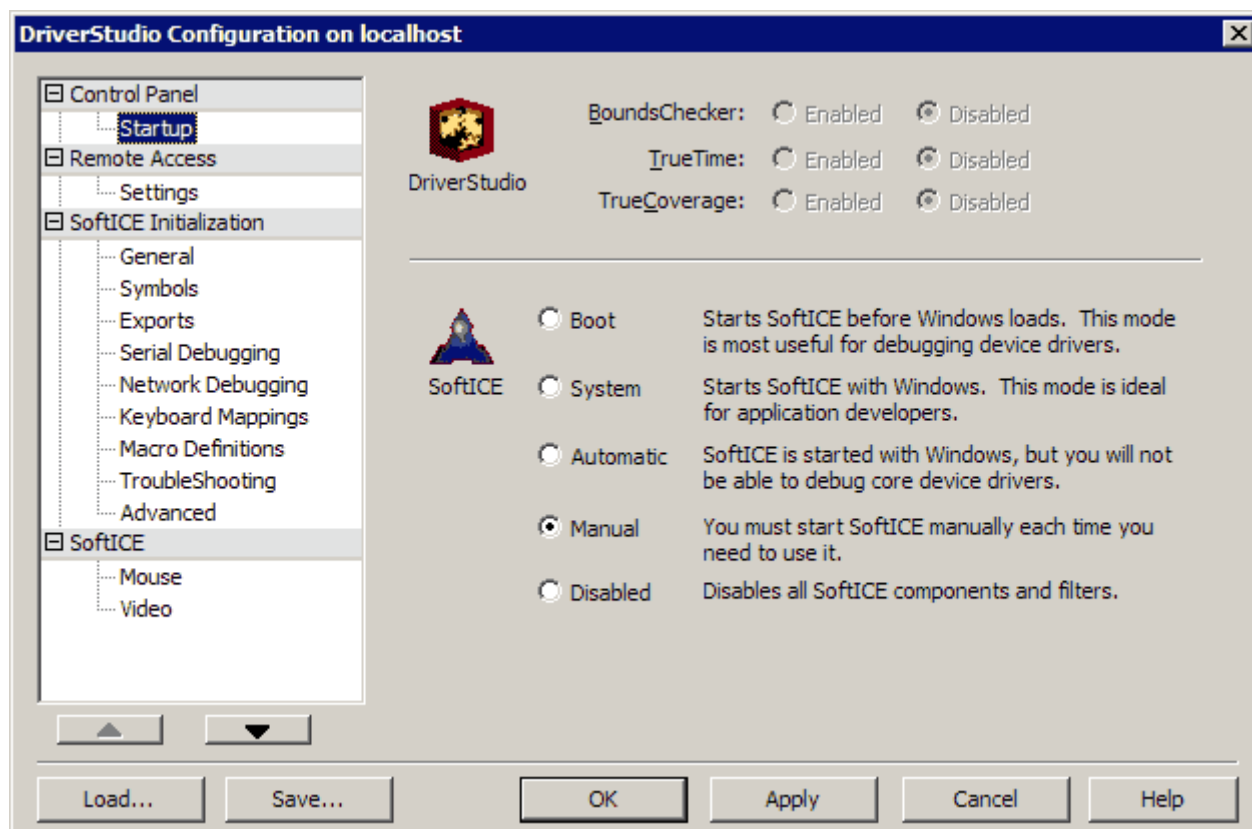
Архив можно взять:

1. <http://reversing.kulichki.net/files/debug/sinstallnt.exe>
2. CRACKL@B CD#1/DVD - <http://cracklab.ru/cd.php>
3. Можно поискать <http://www.yandex.ru/yandsearch?rpt=rad&text=sinstallnt>

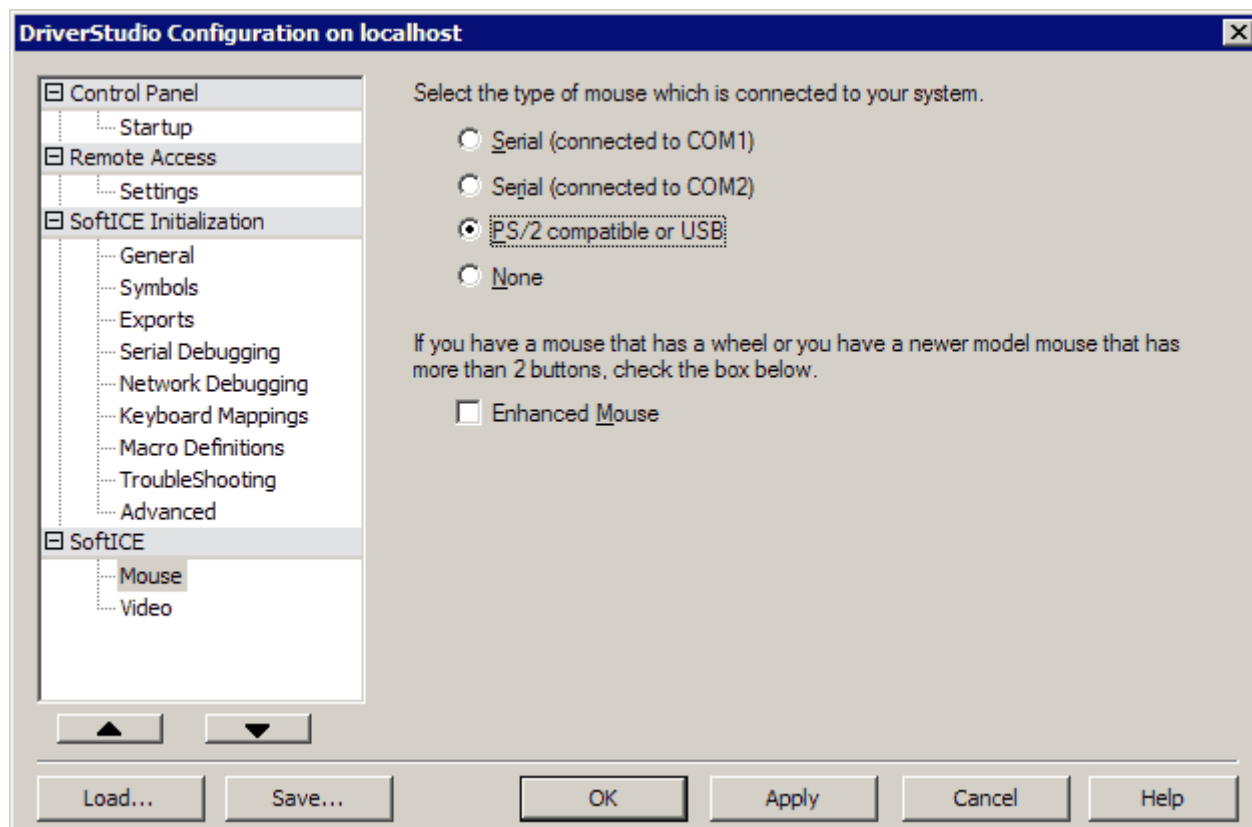
Размер дистрибутива порадует размером в 3 Мб только потому, что .:D.e.M.o.N.i.X:. - создатель сайта <http://reversing.kulichki.net> не поленился сделать свою версию Compuware DriverStudio 2.7, из которой взят только один SoftICE и ничего "лишнего", реальный же размер Compuware DriverStudio 2.7 около 42 Мб.

Опять же, устанавливаю всё "с нуля" и отражу весь процесс установки.

Запускаю установку, ничего примечательного не происходит, пока не появится окно:



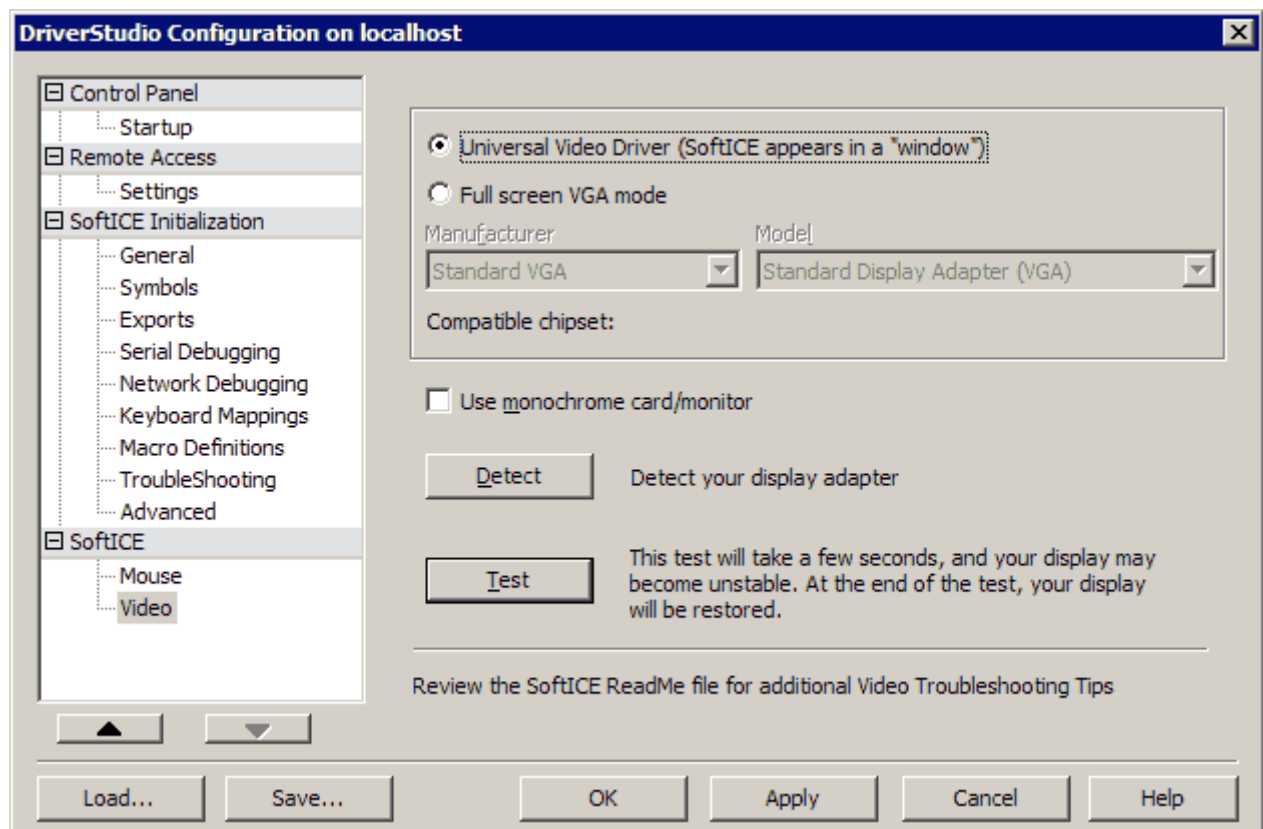
Тут надо опять же выбрать ручной режим запуска отладчика - **Manual**.  
 Далее, самостоятельно переключившись на раскладку **SoftICE - Mouse**,



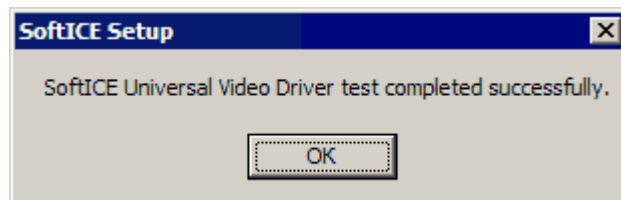
ставлю мой порт мышки - PS/2 и флажок "Enhanced Mouse", так как мышь у меня с

колесиком и 8 кнопками.

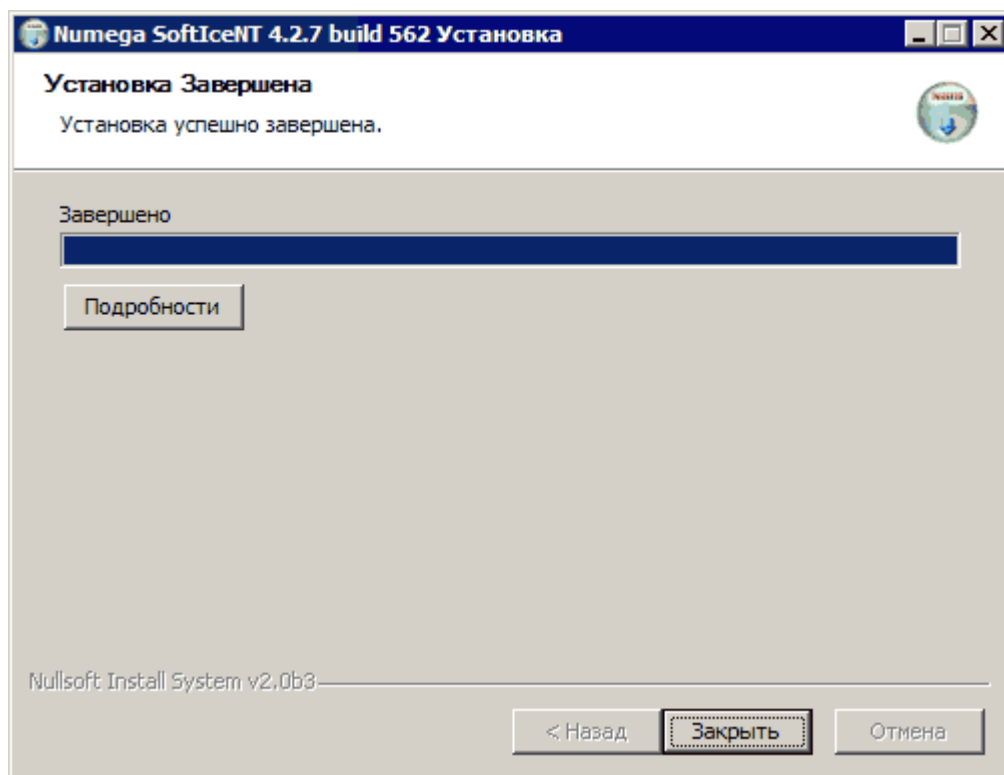
Далее, самостоятельно переключившись на раскладку SoftICE - Video,



оставляю всё как есть и нажимаю Test, вижу что всё в порядке:



Теперь можно нажать кнопки "Apply", "OK", установка завершена:



Есть смысл перезагрузить компьютер, потом пройти в папку C:\program files\SoftIceNT\SoftIce и запустить ntice.bat. Почему именно его - читайте выше, в этой же статье.

Запуск ntice.bat дал незамедлительный результат и SOFTICE запустился, что можно проверить, нажав "Ctrl-D" для вызова окна отладчика. Кроме того, софтайс оказался уже настроенным - размеры окна отладчика нормальные, посмотрю файл winice.dat, находящийся в папке C:\WINDOWS\system32\drivers. Видимо, .:D.e.M.o.N.i.X:. постарался и даже внёс файл настроенный winice.dat в свой релиз SoftICE 4.27.

Настройки инициализации выглядят так:

```
INIT="wl; color f a 4f 1f e; code on; lines 60; wc 32; wd 4; wr; faults off; "  
INIT="ww 4; dex 1 ss:esp; altkey ctrl d; watch es:di; watch eax; watch *es:di; set mouse 3; cls; X;"
```

и немного неосмотрительно удалены все подряд "точки с запятой" для каждой из экспортируемых системных библиотек

```
EXP=\SystemRoot\System32\hal.dll  
EXP=\SystemRoot\System32\ntoskrnl.exe  
EXP=\SystemRoot\System32\ntdll.dll  
EXP=\SystemRoot\System32\kernel32.dll  
EXP=\SystemRoot\System32\user32.dll  
EXP=\SystemRoot\System32\csrssrv.dll  
EXP=\SystemRoot\System32\basesrv.dll  
EXP=\SystemRoot\System32\winsrv.dll
```

Надо сказать, что возможно то что у меня установка прошла без проблем и всё сразу работает лишь частный случай... приведу на всякий случай очень понравившийся мне топик с форума - краткий такой и "по делу":

Gak пишет:

====

отсюда softice 4.2.7

<http://reversing.kulichki.net/files/debug/sinstallnt.exe>

отсюда osinfo.dat (переименовать osinfo\_xpsp1.dat в osinfo.dat и скопировать в %systemroot%\system32\drivers)

<http://reversing.kulichki.net/files/debug/osinfoxpsp1.rar>

отсюда патч дополнения реестра для видео

[http://www.cracklab.ru/f/files/\\_1175709732\\_reg.zip](http://www.cracklab.ru/f/files/_1175709732_reg.zip)

reboot (перезагрузить)

====

Откомментирую теперь: Что касается ссылок, то для ссылки

<http://reversing.kulichki.net/files/debug/osinfoxpsp1.rar> есть теперь копия (на всякий пожарный):

<http://cracklab.ru/download/get.php?g=49>

Для ссылки:

[http://www.cracklab.ru/f/files/\\_1175709732\\_reg.zip](http://www.cracklab.ru/f/files/_1175709732_reg.zip)

копия

<http://cracklab.ru/download/get.php?g=48>

Возможно вам отдельно понадобятся эти два патчика, а может всё и так будет хорошо.

### **ВАРИАНТ 3: Установка SoftICE 4.31 из Compuware DriverStudio 3.1**

Это самая последняя на данный момент версия DriverStudio. Серьёзным минусом этой версии для многих будет размер - 93 Мб урезанная версия (но полнофункциональная), весь пакет DriverStudio (инструмента для разработки драйверов) - 176 Мб минимально.

Найти DriverStudio 3.1 и/или SoftICE 4.31 из DriverStudio 3.1 можно:

1. [http://download.int3.net/debuggers/win\\_debug/DriverStudio.3.1-SoftIce.4.3.1/](http://download.int3.net/debuggers/win_debug/DriverStudio.3.1-SoftIce.4.3.1/) - 93Мб
2. [ftp://ftp.exetools.com/pub/\[NuMega\]/Compuware\\_DriverStudio\\_v3.1-FCN/](ftp://ftp.exetools.com/pub/[NuMega]/Compuware_DriverStudio_v3.1-FCN/) - 181 Мб, однако нужен ещё пароль на ФТП, чтоб скачать оттуда - пароль есть на форуме сайта [www.exetools.com](http://www.exetools.com). У меня не спрашивайте - я не знаю, да и пароль меняют раз в две недели примерно.
3. Ищите ещё ссылки тут:  
<http://www.yandex.ru/yandsearch?text=DriverStudio+3.1&stype=www>
4. Говорят, что DriverStudio 3.1 есть на DVD "AlexSoft SDK и DDK" и на "Золотой Petrosoft на DVD №9".
5. DriverStudio 3.1 есть также на CRACKLAB DVD - <http://cracklab.ru/dvd.php>

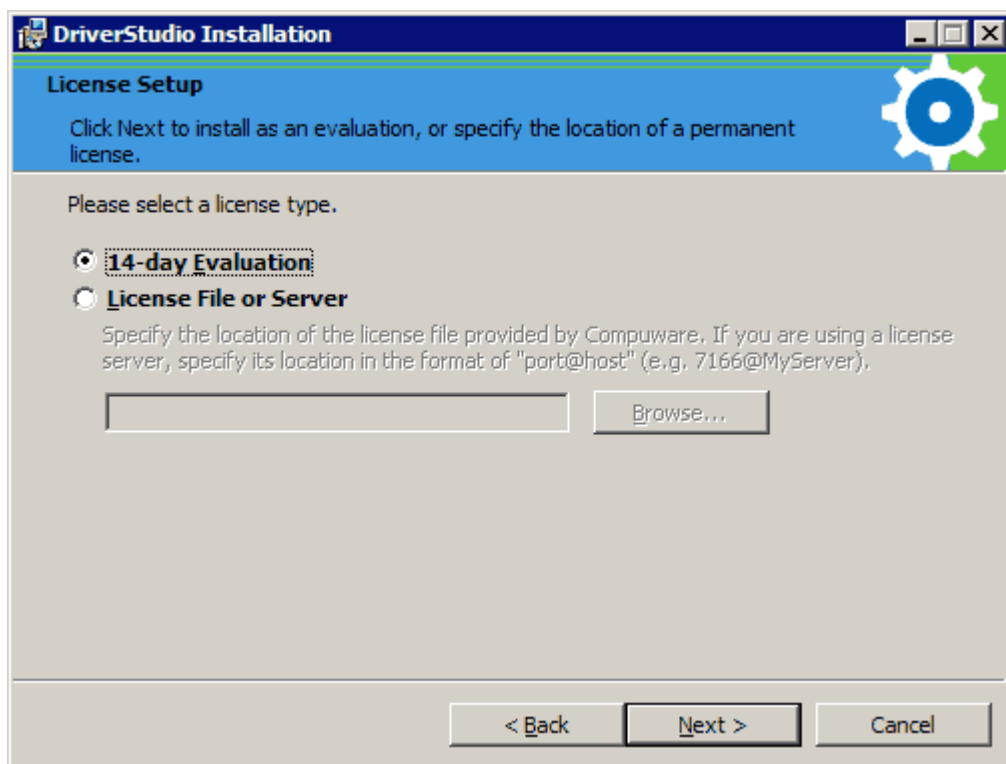
Маловато, конечно, хороших ссылок, но что имеем...

Попробую поставить DriverStudio 3.1, взятый с exetools. Запускаю установку:

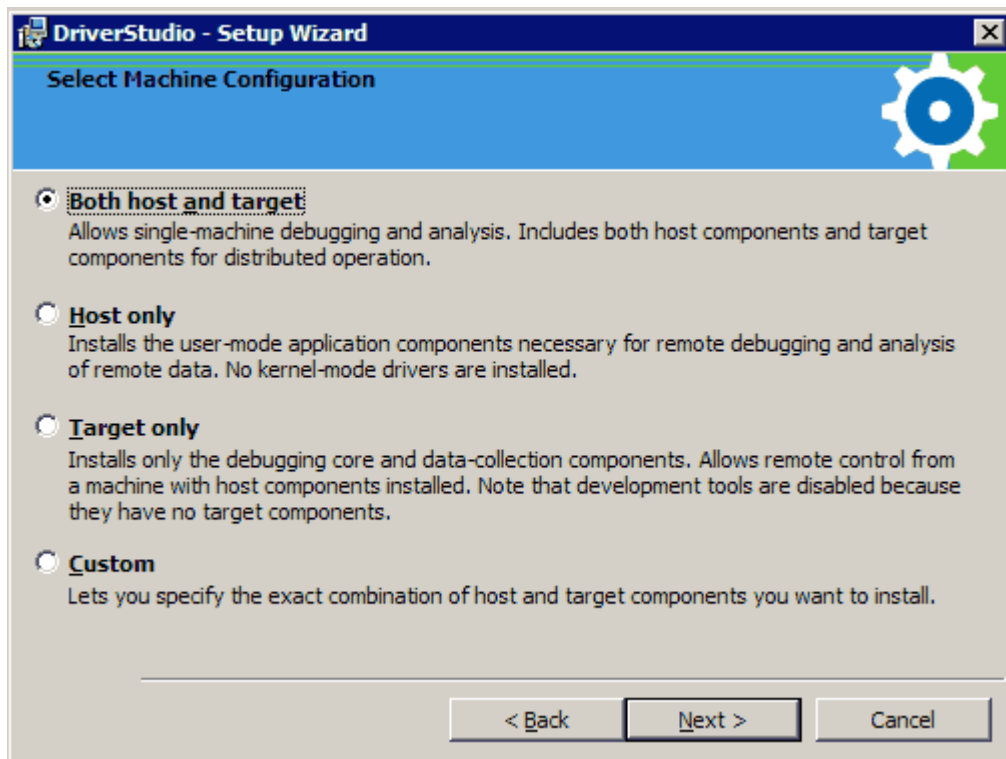


Есть смысл выбрать для установки "Install DriverStudio host and/or target software", потом нужно ввести "правильные" данные в окне:

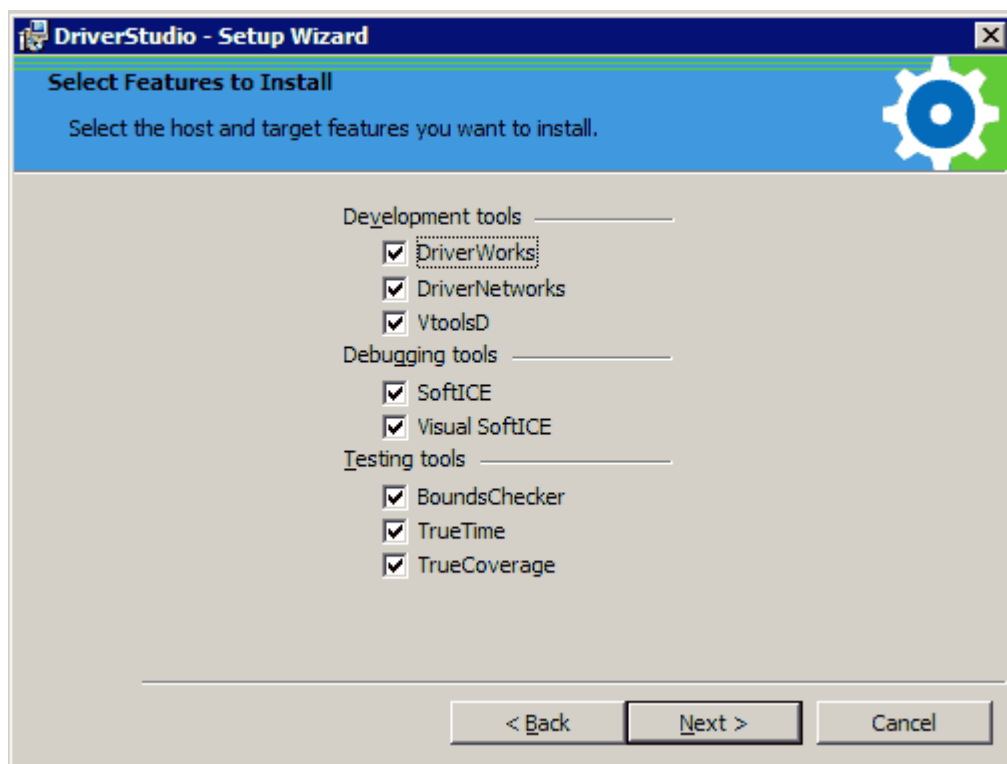
В следующем окне, для начала, я решил выбрать 14-дневный триал, хотя файл studio.dat и прилагается к дистрибу с exetools.



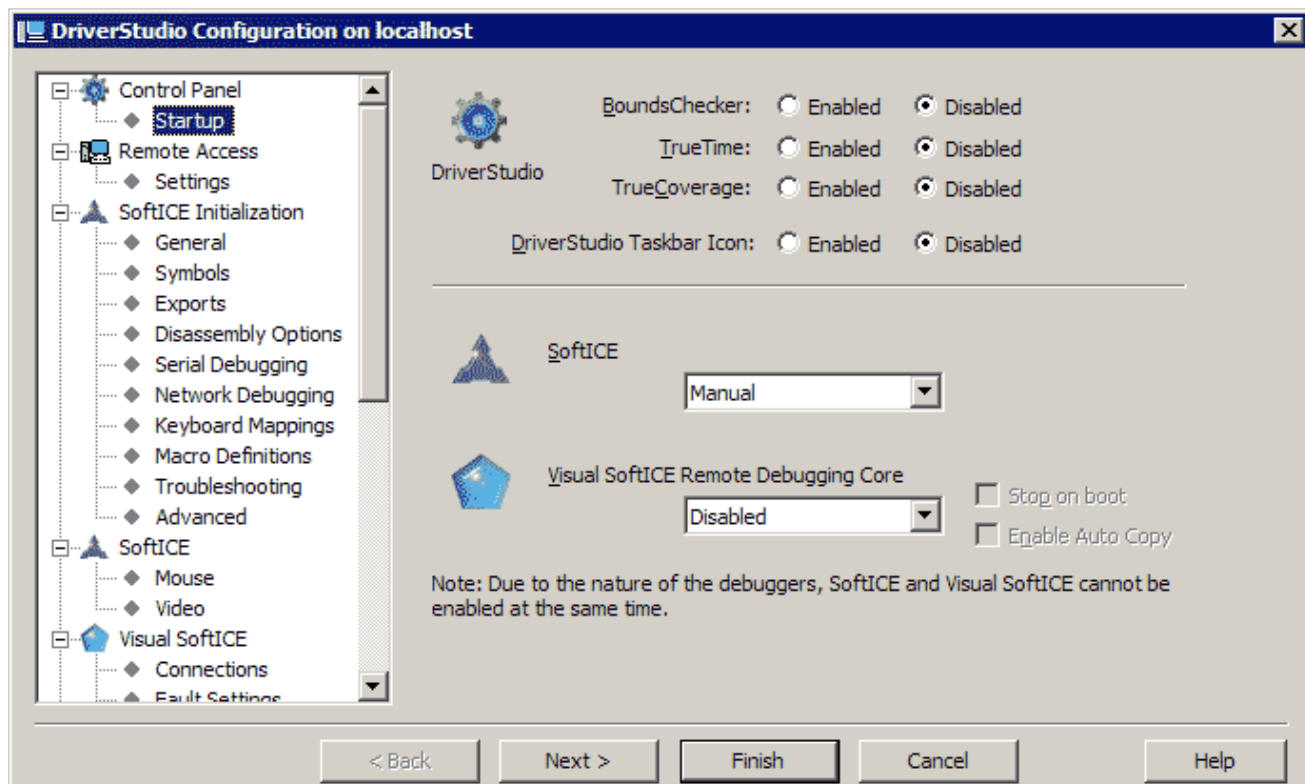
Так как, устанавливаю DriverStudio на один компьютер, выберу пункт "Both host and target" в окне "Select Machine Configuration":



В принципе, в окне "Select Features to Install" можно выбрать только пункт "SoftICE", но возможно остальные инструменты из набора DriverStudio мне тоже не помешают:



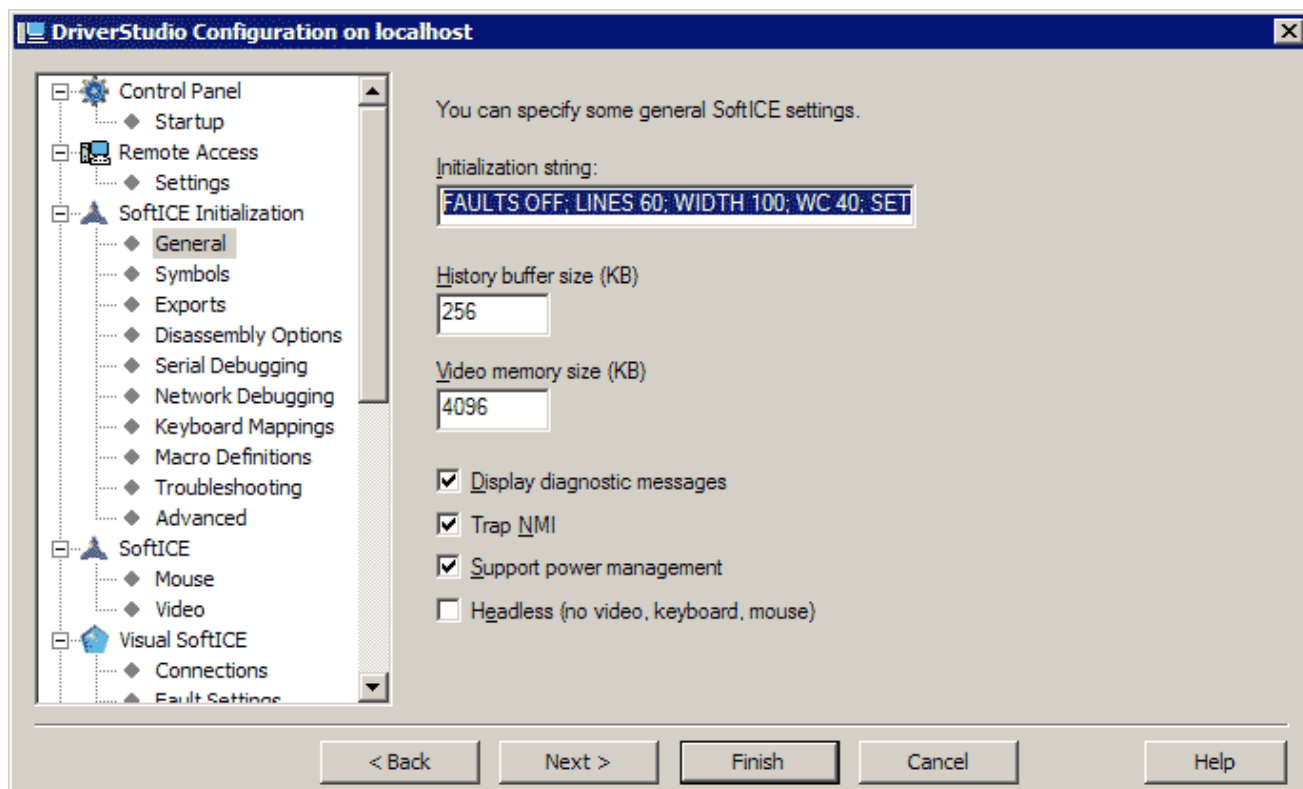
После того, как произошёл процесс установки (копирования файлов) DriverStudio, вылезла программа настройки "DriverStudio Configuration on localhost", теперь нужно произвести все необходимые настройки в этой программе. На вкладке "Control Panel - Startup" ничего трогать не пришлось, однако именно такие настройки я и хотел бы иметь, то есть запуск SoftICE - ручной (Manual), всё остальное отключено. Кстати, эта вкладка программы настройки после завершения установки будет доступна в панели управления: "Пуск" - "Панель управления" - "DriverStudio Config"



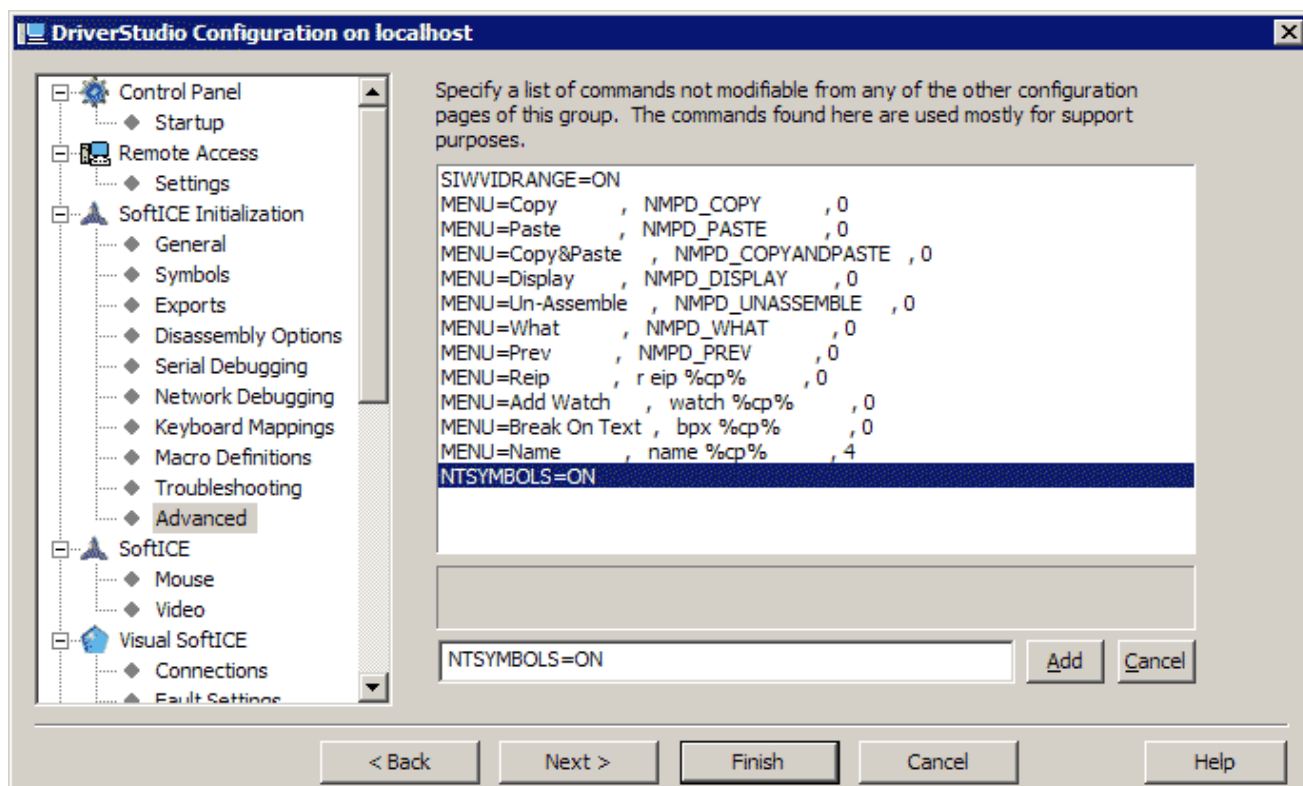
На вкладке "SoftICE Initialization - General" в качестве "Initialization String" я ввёл:

FAULTS OFF; SET BreakInSharedMods ON; LINES 60; WIDTH 100; WC 40; X;

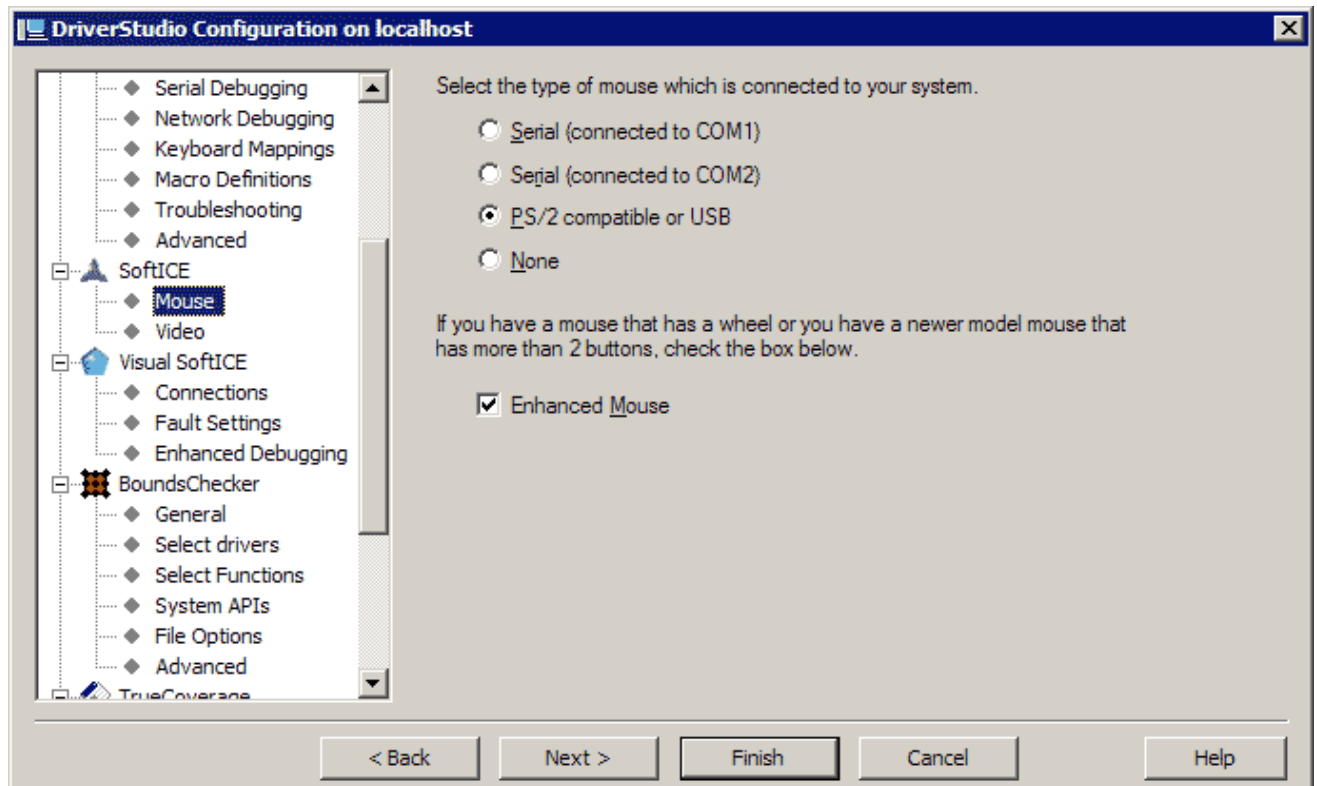
А параметр "Video memory size" увеличен до значения 4096 Кб



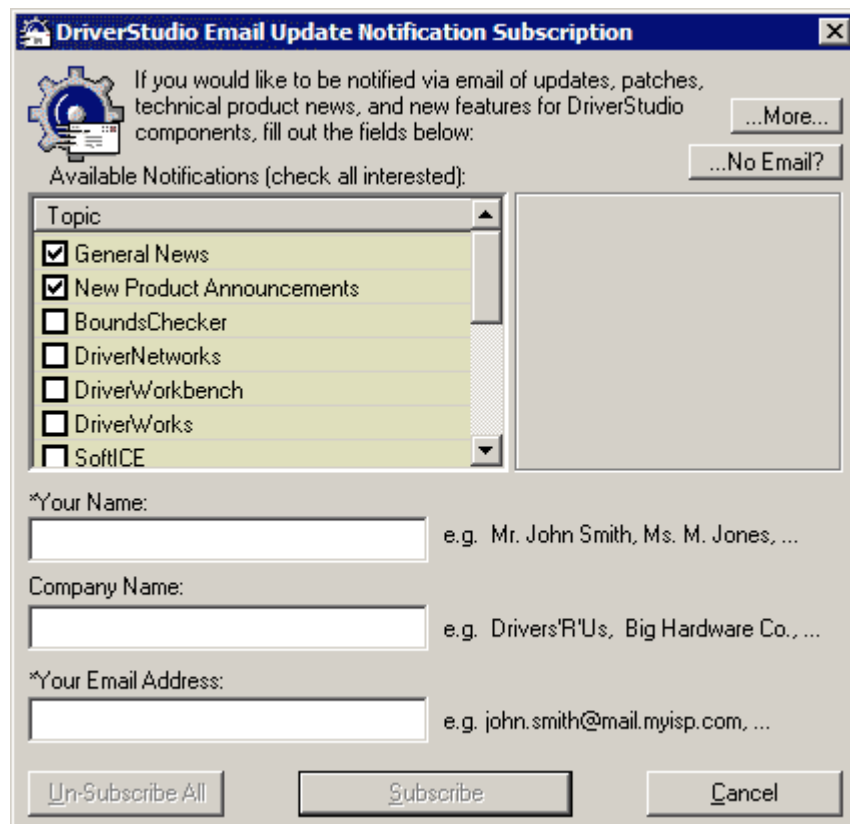
Далее, на вкладке "SoftICE Initialization - Advanced" нужно ввести строчку "NTSYMBOLS=ON" и нажать "Add".



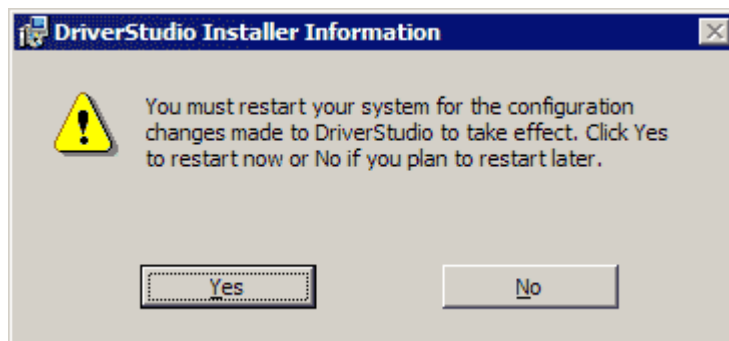
Ну и наконец, на вкладке "SoftICE - Mouse" нужно указать к какому порту подключена мышь и поставить "Enhanced Mouse", если у мыши более 2 кнопок.



Затем нажимаю "Finish" и вижу новое окошко:



Это "заманичивое" предложение меня не заинтересовало, и я нажал "Cancel", после чего было предложено перезагрузить компьютер:



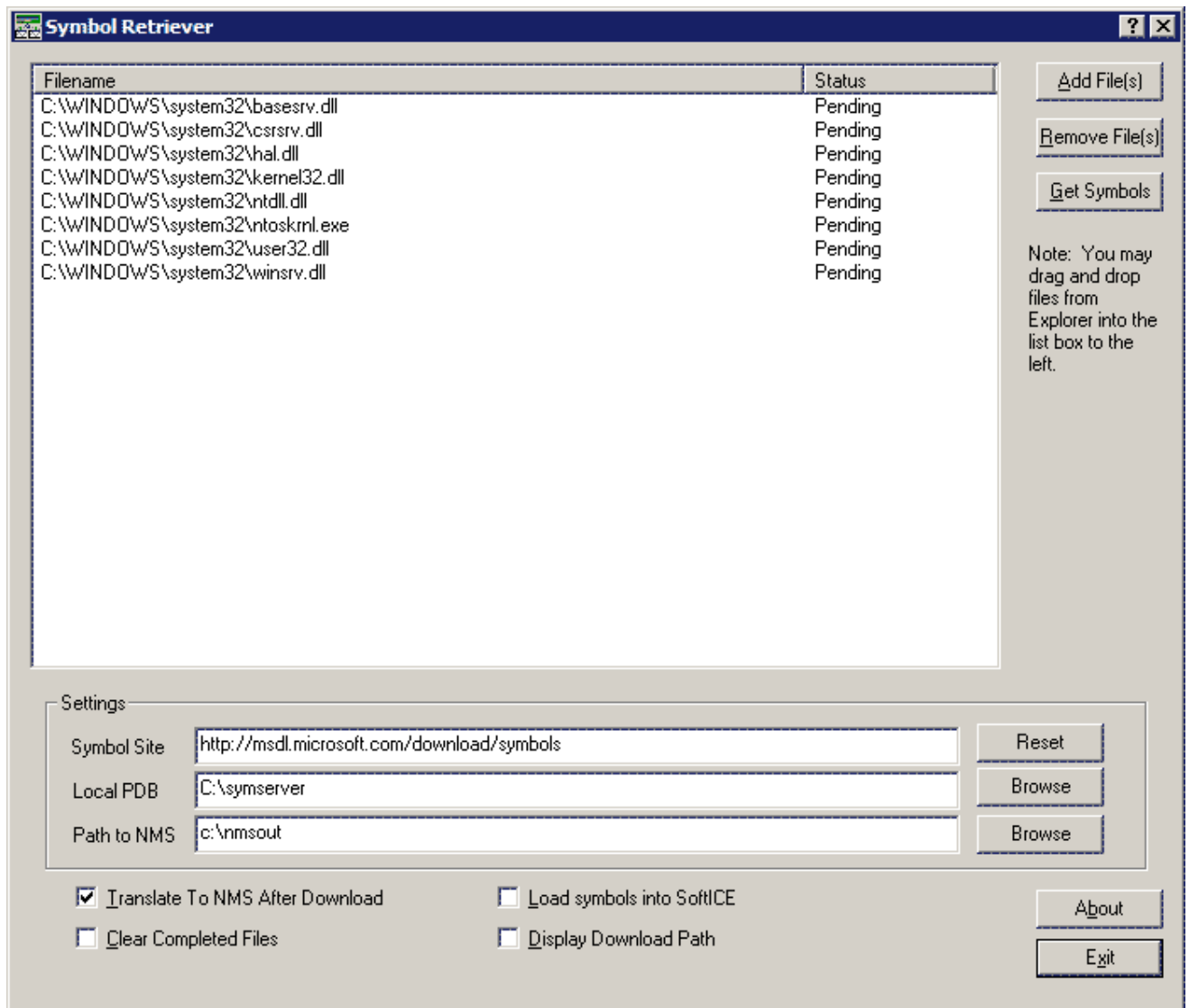
После перезагрузки иду в папку C:\program files\Compuware\DriverStudio\SoftICE и запускаю ntice.bat, который точно также как и в других версиях софтайса запускает службу ntice командой "net start ntice". По нажатию "Ctrl-D" окно софтайса появилось, теперь посмотрим файл C:\WINDOWS\system32\drivers\Winice.dat

Как обычно, сверим наличие этих файлов:

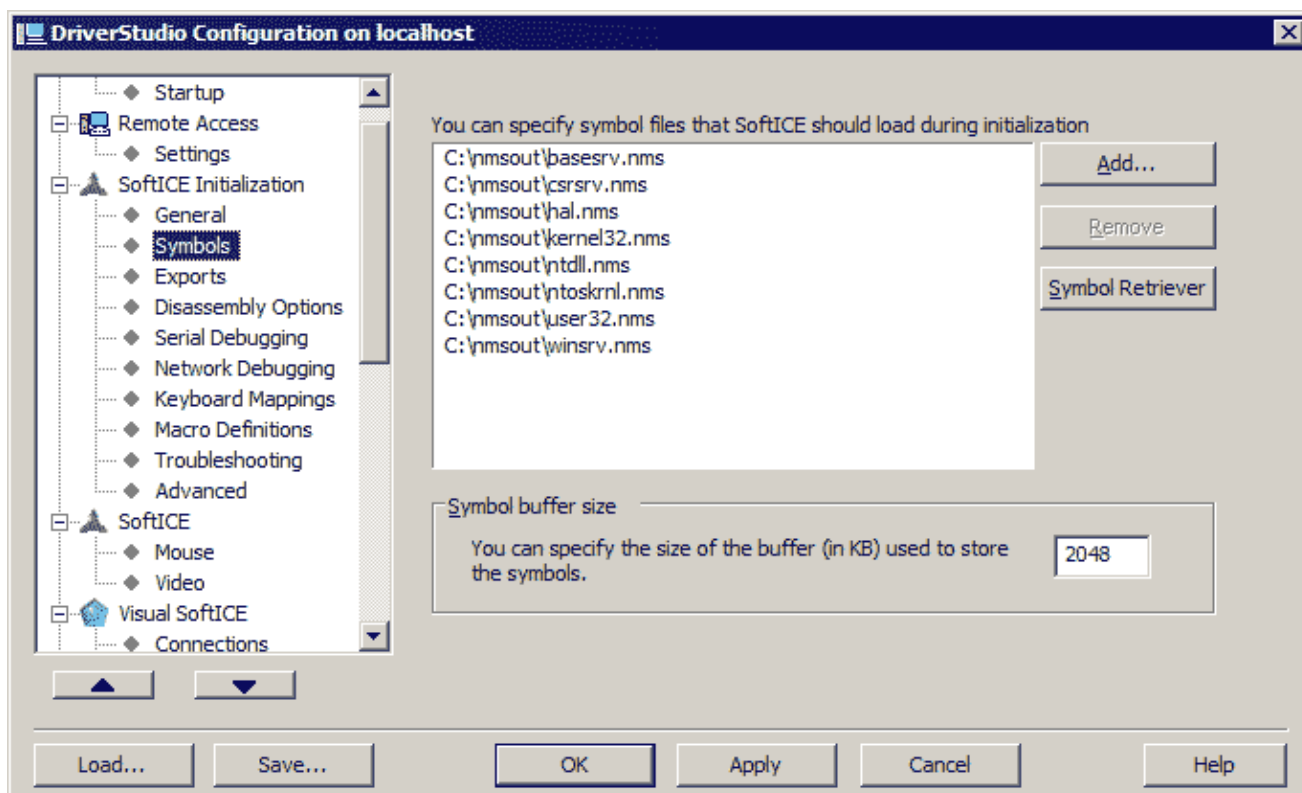
```
; Change the path to the appropriate drive and directory
; EXP=\SystemRoot\System32\hal.dll
; EXP=\SystemRoot\System32\ntoskrnl.exe
; EXP=\SystemRoot\System32\ntdll.dll
; EXP=\SystemRoot\System32\kernel32.dll
; EXP=\SystemRoot\System32\user32.dll
; EXP=\SystemRoot\System32\csrssrv.dll
; EXP=\SystemRoot\System32\basesrv.dll
; EXP=\SystemRoot\System32\winsrv.dll
```

и уберём "точку с запятой" перед теми строками, файлы из которых существуют у вас на машине, также можно заодно и выполнить рекомендацию и заменить \SystemRoot\ на C:\WINDOWS\system32\ в этих строках. Также, на форуме я нашёл совет - скачать отладочные символы для всех этих библиотек. Для этого нужно запустить Symbol Retriever, находящийся по адресу C:\program files\Compuware\DriverStudio\SoftICE\SymbolRetriever\symrtrvr.exe, нажав кнопку "Add File(s)" выбираю все вышеуказанные библиотеки:

```
hal.dll
ntoskrnl.exe
ntdll.dll
kernel32.dll
user32.dll
csrssrv.dll
basesrv.dll
winsrv.dll
```



Теперь нужно подключиться к Интернет и нажать кнопку "Get Symbols", отладочные символы скажутся (около 8 Мб) и отконвертируются в подходящий для отладчика SoftICE формат - \*.nms, файлы будут находиться в указанной папке - в данном случае в c:\nmsout, после этого запускаю уже знакомую программу настройки "DriverStudio Configuration on localhost", которая лежит по адресу C:\program files\Compuware\DriverStudio\Common\Bin\DSConfig.exe. На вкладке "SoftICE Initialization - Symbols", используя кнопку "Add", добавляю все полученные ранее \*.nms файлы, размер которых в общей сложности составляет у меня 1,72 Мб, поэтому параметр "Symbol buffer size" я решил увеличить с 512 до 2048 Кб.



Далее нажимаю "Apply", "OK".

Теперь выполняю ещё одну рекомендацию с форума и скачаю файл OSINFO.DAT с официального сайта производителя - Compuware.

Если на компе установлена Windows XP SP1 (обычная Windows XP), то качать надо:

[ftp://ftp.compuware.com/pub/driverstudio/outgoing/OsInfo/osinfo\\_XPSP1.dat](ftp://ftp.compuware.com/pub/driverstudio/outgoing/OsInfo/osinfo_XPSP1.dat)

а если установлен второй сервис пак (Windows XP SP2), то качать надо:

<ftp://ftp.compuware.com/pub/driverstudio/outgoing/OsInfo/OSINFO.DAT>

В первом случае нужно будет переименовать скачанный файл osinfo\_XPSP1.dat в OSINFO.DAT. Теперь новым, только что скачанным, файлом OSINFO.DAT нужно заменить одноименный файл, находящийся в папке C:\WINDOWS\system32\drivers\

Перезагружаю компьютер, запускаю ntice.bat, вызываю SoftICE нажатием "Ctrl-D" и пробую установить прерывание для проверки работоспособности отладчика - ввожу команду, например bpx GetWindowTextA - у меня всё работает. Выхожу из консоли SoftICE нажатием "Ctrl-D" - вот и всё ! Можно работать !

Надеюсь, эта статья окажется вам полезной. Вероятно, могут возникнуть какие-то нетривиальные проблемы при установке софтайса и естественно у вас появится желание задать вопрос по каждой такой проблеме мне по email - [bad\\_guy@cracklab.ru](mailto:bad_guy@cracklab.ru), однако, я прошу вас этого не делать, потому как я не являюсь всё-таки экспертом в установке софтайс. Советую обратиться на форум CRACKL@B - <http://cracklab.ru/f/> и задать свой вопрос широкому кругу крэкеров, потому как вероятность того, что хотя бы один из участников форума сталкивался с такой же как у вас проблемой гораздо выше, чем вероятность того, что я один могу ответить на ваш вопрос.

При написании данной статьи я активно пользовался архивом форума CRACKL@B - <http://cracklab.ru/f/>, рассматривая и анализируя старые топики форума. Хочу выразить благодарность всем тем участникам форума, кто смог дать вразумительные советы по установке софтайс тем, у кого возникали вопросы. Особо помогли в написании материалы

посты от: Ara, dragon, Man1ac, Bitfry, nice, WELL (особое спасибо за выложенный на [download.int3.net](http://download.int3.net) SoftICE 4.31 из DS 3.1).

Удачи вам в вашей деятельности, чем бы вы ни занимались, Bad\_guy.

---

Материалы находятся на сайте <http://cracklab.ru/art/>