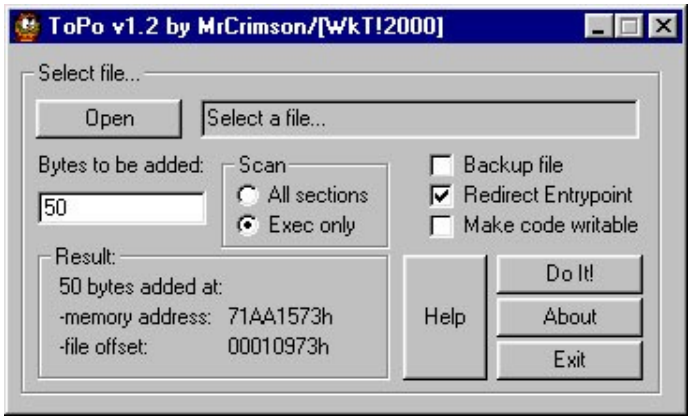
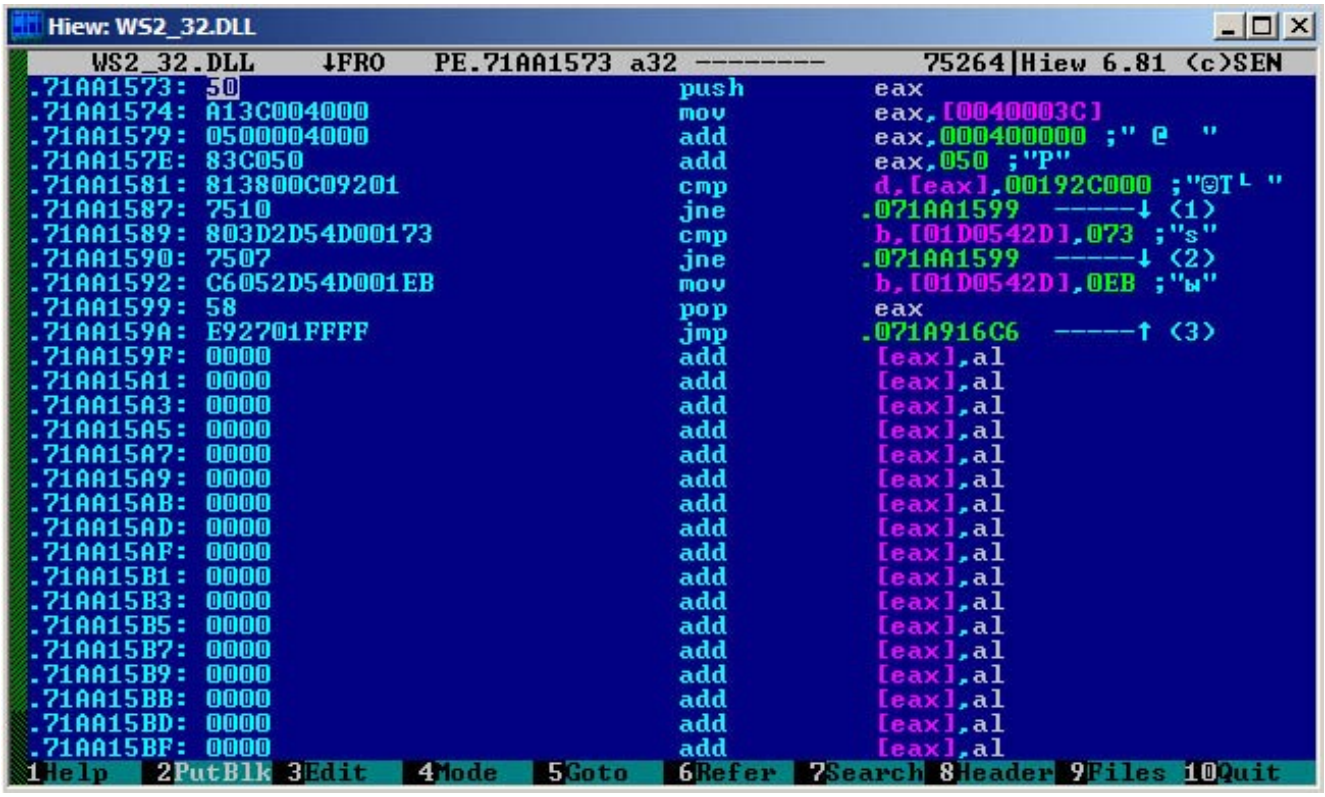
Inline patching SAMInside v2.6.5.0

1. Прежде всего необходимо найти байтики, которые нужно изменить, чтобы очитить black list. Я не буду подробно на этом останавливаться, всё понятно из ролика loader.flv
2. **Maximus** описал в свой статье метод инлайн патча, но то же самое можно сделать проще: нетрудно заметить, что перед появлением сообщения *“Asprotect.dll расположена в памяти по адресу…”* программа загружает библиотеку WS2_32.DLL , вот её-то мы и будем патчить :-)
3. Прежде всего надо скопировать этот файл из папки Windows\system32 в папку с программой.
4. Теперь воспользуемся утилитой ToPo v1.2 для того, чтобы сделать инлайн патч:



5. Теперь открываем файл WS2_32.DLL в HiEW переходим на смещение 10973h и пишем код патча:



Тут требуются некоторые пояснения (спасибо **ClockMan**'у за подсказку !): прежде всего необходимо убедиться, что мы собираемся патчить именно тот файл, для этого надо сравнить его Image Size с правильным.
Чтобы понять, как его (Image Size) найти, надо почитать про формат PE файлов, например здесь: http://www.emanual.ru/download/www.eManual.ru_1298.html
Откуда я узнал, что правильный Image Size = 192C000 ? Его можно посмотреть в любом редакторе PE файлов (LordPE или PE Tools) или дойти до него самостоятельно: открываем файл SAMInside.exe в HiEW идём на смещение 3Ch и видим там 10 01 00 00 то есть 110 задом наперёд, идём на смещение 160h (110+50) и видим 00 C0 92 01 то есть 192C00 :-)
Если файл правильный – проверяем, что по смещению находятся нужные нам байты и, если они на месте, - патчим:

```
.71AA1573: 50              push  eax                ; Сохраняем EAX
.71AA1574: A13C004000      mov   eax,[0040003C]     ; Получаем указатель на PE
.71AA1579: 0500004000      add   eax,000400000      ; Прибавляем Image Base
.71AA157E: 83C050          add   eax,050            ; Прибавляем Base
.71AA1581: 813800C09201    cmp   d,[eax],00192C000  ; Сравниваем Image Size с правильным
.71AA1587: 7510            jne   .071AA1599         ; Не оно – на выход
.71AA1589: 803D2D54D00173  cmp   b,[01D0542D],073   ; Проверяем байты по нужному смещению
.71AA1590: 7507            jne   .071AA1599         ; Не то – на выход
.71AA1592: C6052D54D001EB  mov   b,[01D0542D],0EB   ; Патчим
.71AA1599: 58              pop   eax                ; Восстанавливаем EAX
.71AA159A: E92701FFFF      jmp   .071A916C6         ; Прыжок на OEP
```

6. Всё, теперь можно положить файл SAMInside.key с забаненным серийным номером в папку с программой и убедиться, что программа его принимает :-) И что характерно, сам файл SAMInside.exe остался нетронутым, соответственно, нет необходимости патчить проверку CRC ;-)