

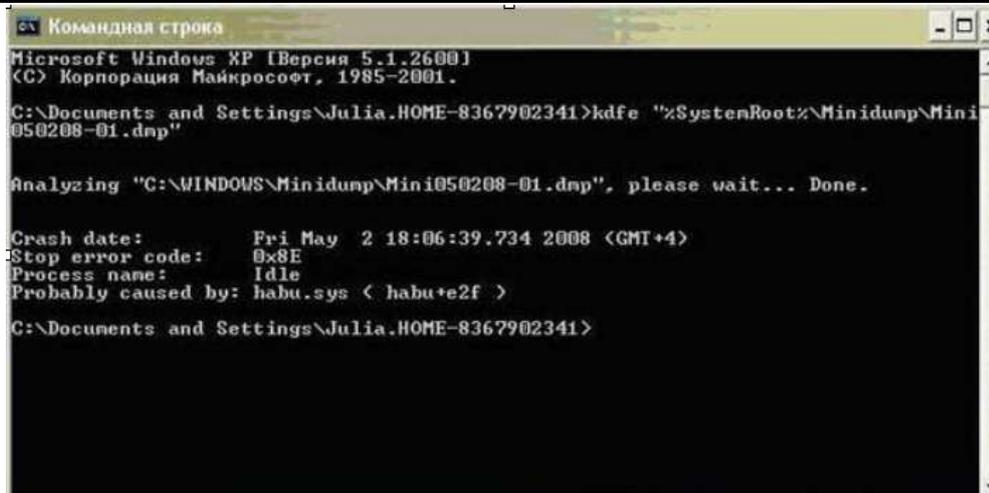
Анализ дампов BSOD самостоятельно.

Если по каким-то причинам Вы не хотите обратиться за анализом дампов ко мне или к моим специалистам (см.выше по тексту), то можете проанализировать их сами. Т.к. наиболее частой причиной являются именно драйвера, то разбор и анализ дампа позволит выявить Вам сбоящий драйвер и обновить/откатить его на более новую/старую стабильную версию, которая не вызывает ошибок и синих экранов. Как посмотреть содержимое дампа **bsod** (два способа):

Способ Первый. Довольно старый и долгий, но в общем-то довольно эффективный и проверенный временем – это пакет **debugging+kdfe**.

Как поставить и что делать:

- Загрузите и установите – [Debugging Tools for Windows](#).
- [Загрузите сценарий](#) (kdfe.cmd). Этот файл нужно извлечь из архива в папку **System32**.
- Все, что осталось – открыть командную строку и написать там **kdfe “%systemroot%\Minidump\Mini050208-01.dmp”** где **Mini050208-01.dmp** – имя файла из папки **Minidump**. Путь можно указывать без кавычек. Само собой, что Вы, естественно, вместо этого имени файла подставляете имя своего. Папка тоже может быть другой, особенно, если дампы где-то скачали. Собственно, я создал себе папку **bsod** на диске и туда кидаю все дампы, а в пути консоли, соответственно, пишу **kdfe C:\bsod\имя_дампа.dmp**. Потом нажимаете **Enter** и через некоторое время получаете имя повинного в ваших проблемах драйвера. Скриншот с пояснением:



```
Командная строка
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\Julia.HOME-8367902341>kdfe "%SystemRoot%\Minidump\Mini050208-01.dmp"

Analyzing "C:\WINDOWS\Minidump\Mini050208-01.dmp", please wait... Done.

Crash date:      Fri May  2 18:06:39.734 2008 <GMT+4>
Stop error code:  0x8E
Process name:    Idle
Probably caused by: habu.sys < habu+e2f >

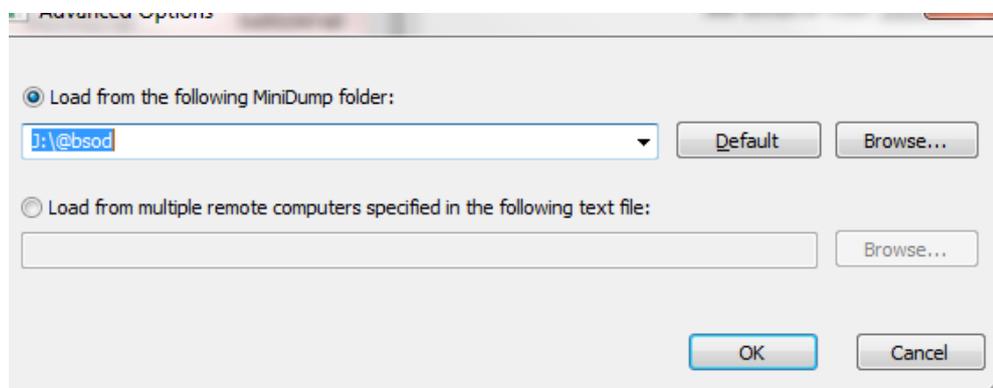
C:\Documents and Settings\Julia.HOME-8367902341>
```

Нам важна строчка **probably caused by:** в которой и указан виновник синего экрана смерти. На скриншоте мы видим, что в данном случае виноват некий драйвер **habu.sys**, а посему нам необходимо найти в поисковых системах что это за драйвер, а так же скачать обновления к нему или более старую стабильную версию. В данном случае это драйвер **USB-мыши (Razer Habu)**. Соответственно, совет по устранению bsod'a – это переустановить драйвер на более новый или хотя бы попробовать просто переустановить тот, что есть.

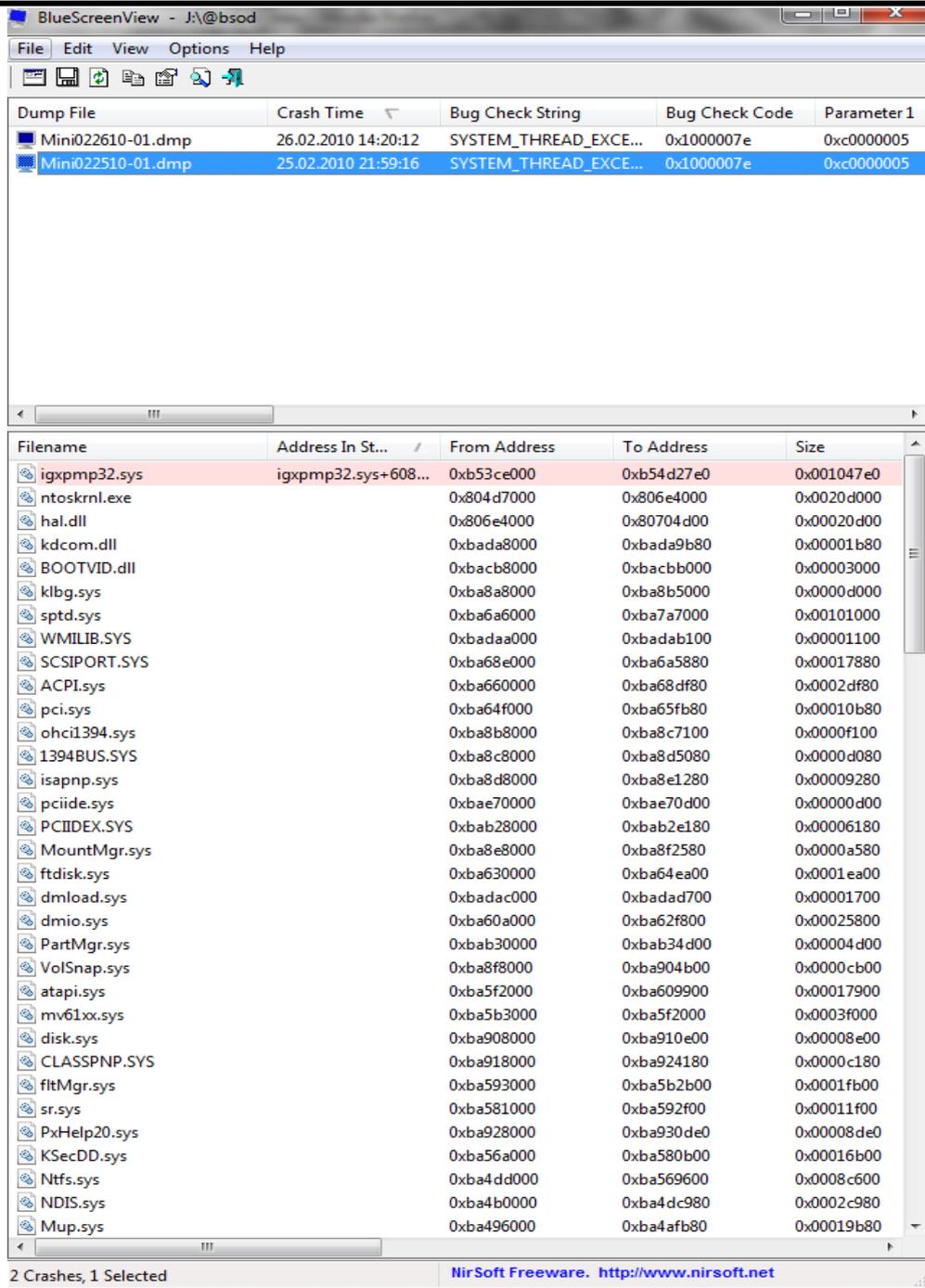
Зачастую бывает необходимо еще поглядывать на строчку **process** ибо там бывает указан **.exe** (или **.dll** и тп) файл какой-либо программы или её части, т.е составляющего куска антивирусника\фаерволла и тогда проблема скорее в нем, а не в драйвере. Соответственно, если Вы увидели подобное, то для устранения синего экрана рекомендуется переустановить\сменить антивирус\фаерволл. К слову, почти все антивирусы подгружают свои драйвера, поэтому “кусочек” антивируса может засветится и в строчке **probably caused by**:

Способ второй. Штука с говорящим названием **BlueScreenView**. Собственно, это программка для анализа дампов. Полностью бесплатна и даже несколько поудобнее чем консольный способ выше, ибо показывает быстрее, а так же можно переключаться между дампами, не вводя постоянно их название руками.

После запуска увидите окно программы, где надо будет в настройках указать папку куда Вы складываете дампы. Для этого тыркаетесь в **Options – Advanced Options**, и укажите папку с дампами.



После указания папки скопируйте туда (если там их нет изначально) дампы и нажмите в кнопку “**Обновить**” (Refresh) в программе. Потом выделяете название нужного дампа и видите драйвер-виновник синего экрана (или несколько). Они обычно выделены программой красным цветом.



Дальнейшая процедура такая же как и в первом случае – идем искать что это за драйвер, от какого устройства, а так же скачивать-устанавливать-переустанавливать оный. Преимущество второго способа (т.е программы BlueScreenView) в том, что он шустрее, удобней, иногда точнее и порой показывает несколько виноватых драйверов, вместо одного.

Если Вы ничего не поняли или возиться с анализом у Вас нет времени, то мы всегда ждем Вас у нас на форуме или у меня в **bsod**-почте (см.выше по тексту в подразделе “Поддержка по решению проблем с BSOD”)