



**Dr.WEB®**

**Shark**

**Руководство Пользователя**

## **© 2008 ООО "Доктор Веб". Все права защищены.**

Материалы, приведенные в данном документе, являются собственностью ООО "Доктор Веб" и могут быть использованы исключительно для личных целей приобретателя продукта. Ни какая часть данного документа не может быть скопирована, размещена на сетевом ресурсе или передана по каналам связи и в средствах массовой информации или использована любым другим образом кроме использования в личных целях без ссылки на источник.

### **ТОРГОВЫЕ ЗНАКИ**

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt! и логотипы Dr.WEB и Dr.WEB INSIDE являются зарегистрированными товарными знаками ООО "Доктор Веб". Иные зарегистрированные товарные знаки, логотипы и наименования компаний, упомянутые в данном документе, являются собственностью их владельцев.

### **ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ**

Ни при каких обстоятельствах ООО "Доктор Веб" и его поставщики не несут ответственности за ошибки и/или упущения, допущенные в данном документе и понесенные в связи с ними убытки приобретателя продукта (прямые или косвенные, включая упущенную выгоду).

## **Dr.Web Shark Руководство Пользователя 18.11.2008**

ООО "Доктор Веб", Центральный офис в России  
125124  
Россия, Москва  
3-я улица Ямского поля, вл.2, корп.12А

Веб-сайт: [www.drweb.com](http://www.drweb.com)  
Телефон: +7 (495) 789-45-87

Информацию о региональных представительствах и офисах Вы можете найти на официальном сайте компании.

# **ООО "Доктор Веб"**

ООО "Доктор Веб" - российский разработчик средств информационной безопасности.

Компания предлагает эффективные антивирусные и антиспам-решения как для государственных организаций и крупных компаний, так и для частных пользователей.

Антивирусные продукты ООО "Доктор Веб" разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ и соответствуют мировым стандартам безопасности.

Сертификаты и награды, а также обширная география пользователей свидетельствуют об исключительном доверии к продуктам компании.

**Мы благодарны пользователям за поддержку решений семейства ООО "Доктор Веб"!**



# Содержание

<b>Глава 1. Предисловие Dr.Web Shark</b>	<b>6</b>
Используемые обозначения	6
Техническая поддержка	8
Режимы работы	8
<b>Глава 2. Начало работы</b>	<b>10</b>
Лицензирование	10
Установка	10
Запуск Dr.Web Shark	11
Мастер Dr.Web Shark	11
<b>Глава 3. Консоль Dr.Web Shark</b>	<b>14</b>
Меню	15
Панель инструментов	15
<b>Вкладки отчетов</b>	<b>16</b>
Вкладка Processes	16
Вкладка SSDT	18
Вкладка Drivers	20
Вкладка Startups	22
<b>Дополнительные инструменты</b>	<b>23</b>
Инструмент File Browser	24
Инструмент MBRs Browser	25
<b>Глава 4. Нейтрализация угроз</b>	<b>28</b>
Управление процессами	28
Управление системными сервисами	29



<b>Управление драйверами</b>	<b>31</b>
<b>Управление файлами</b>	<b>32</b>
<b>Создание дампов памяти</b>	<b>34</b>
<b>Глава 6. Генерация отчетов</b>	<b>37</b>



# Глава 1. Предисловие Dr.Web Shark

**Dr.Web Shark** - это бесплатная утилита **ООО "Доктор Веб"**, которая собирает и анализирует информацию о компьютере и позволяет обнаруживать неизвестные вредоносные программы. В отличие от антивирусных сканеров, **Dr.Web Shark** не проверяет отдельные файлы, а так же не требует для работы баз с вирусными сигнатурами. Для обнаружения новых, ранее не встречавшихся вредоносных программ **Dr.Web Shark** анализирует изменения объектов операционной системы, гарантированный доступ к которым обеспечивается применением технологий **Dr.Web Shield**.

**Dr.Web Shark** собирает информацию о следующих объектах:

- [процессах](#), выполняемых операционной системой;
- [записях в таблице системных вызовов](#) System Service Descriptors Table;
- [драйверах](#), установленных в системе;
- [объектах автозапуска](#).

Также утилита предоставляет дополнительные инструменты [File Browser](#) и [Master Boot Records \(MBRs\) Browser](#) для анализа файловой системы и загрузочных записей.

С помощью **Dr.Web Shark** вы можете не только обнаруживать вредоносные программы, но и [нейтрализовывать](#) последствия их работы.

## Используемые обозначения

В данном руководстве применены следующие условные обозначения ([табл. 1](#)).



Таблица 1. Условные обозначения

Convention	Description
<b>Полужирный</b>	Названия кнопок и других элементов пользовательского интерфейса, а так же данные, необходимые вам необходимо ввести именно так, как они приведены в руководстве.
<b>Зеленый полужирный</b>	Названия продуктов компании <b>ООО "Доктор Веб"</b> и их компонентов.
<u>Зеленое подчеркивание</u>	Ссылки на разделы документа и веб-сайты.
<i>Ёóðÿá</i>	Текст-заменитель информации, которую вам нужно ввести. В примерах ввода команд такое выделение указывает на участки команды, которые вам необходимо заменить актуальным значением. Так же может выделять термины.
ПРОПИСНЫЕ БУКВЫ	Названия клавиш клавиатуры.
Символ "плюс" (+)	Указывает на одновременное нажатие нескольких клавиш. Например, запись ALT+F1 обозначает, что необходимо нажать клавишу F1, удерживая нажатой клавишу ALT.
Восклицательный знак	A Важные замечания и указания.



## Техническая поддержка

Страница службы технической поддержки ООО «Доктор Веб» находится по адресу <http://support.drweb.com/>.

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в отдел технической поддержки, рекомендуется попробовать найти решение одним из следующих способов:

- ознакомиться с последними версиями описаний и руководств по адресу <http://download.drweb.com/>;
- прочитать раздел часто задаваемых вопросов по адресу <http://support.drweb.com/>;
- попытаться найти ответ в базе знаний Dr.Web по адресу <http://wiki.drweb.com/>;
- посетить форумы Dr.Web по адресу <http://forum.drweb.com/>.

Если после этого вам не удалось решить проблему, то вы можете воспользоваться одним из следующих способов, чтобы связаться со службой технической поддержки:

- заполнить веб-форму вопроса в соответствующей секции раздела <http://support.drweb.com/>;
- написать электронное письмо по адресу [support@drweb.com](mailto:support@drweb.com);
- позвонить по телефону в Москве: +7 (495) 789-45-87.

Найти ближайшее к вам представительство ООО «Доктор Веб» и всю контактную информацию, необходимую пользователю, вы можете по адресу <http://company.drweb.com/contacts/moscow>.

## Режимы работы

**Dr.Web Shark** поддерживает следующие режимы работы:

- интерактивный режим;
- режим генерации отчета.





### Интерактивный режим

Для работы в этом режиме используется [консоль](#) Dr.Web Shark, которая отображает информацию об операционной системе в режиме реального времени (динамический отчет). Консоль так же предоставляет средства по нейтрализации обнаруженных вредоносных программ и восстановлению модифицированных ими характеристик системы.

В это режиме вы можете:

- [просматривать](#) и [управлять](#) системными процессами;
- [просматривать](#) and [управлять](#) содержимым таблицы системных вызовов System Service Descriptors Table;
- [просматривать](#) and [управлять](#) установленным драйверами;
- [просматривать](#) список объектов автозапуска;
- [просматривать](#) и [управлять](#) объектами файловых систем;
- [просматривать](#) информацию о загрузочных записях дисков.

Также вы можете сохранить информацию в виде статического отчета.

### Режим генерации отчета

В этом режиме работы сбор данных осуществляется в фоновом режиме и завершается формированием статического отчета. Консоль Dr.Web Shark не отображается. Вы можете использовать этот режим, если анализ состояния системы осуществляется удаленно (например, специалистами [службы технической поддержки](#) ООО «Доктор Веб»).

Содержимое статических отчетов не зависит от режима работы приложения, но, в отличие от интерактивного режима, в режиме генерации отчетов недоступны функции управления объектами операционной системы.



## Глава 2. Начало работы

Чтобы начать работу с утилитой **Dr.Web Shark**, выполните следующие шаги:

1. Запустите приложение.
2. Выберите режим работы:
  - если вы собираетесь воспользоваться помощью специалистов службы технической поддержки ООО «Доктор Веб», создайте и отправьте по электронной почте отчет Dr.Web Shark;
  - если вы хотите самостоятельно проанализировать работу операционной системы в режиме реального времени, откройте консоль Dr.Web Shark.
3. После проведения анализа, нейтрализируйте обнаруженные угрозы.

## Лицензирование

**Dr.Web Shark** - это бесплатная утилита для обнаружения вредоносных программ. Вы можете использовать **Dr.Web Shark** как отдельное приложение, так и в дополнение к другим антивирусным продуктам ООО "Доктор Веб". Лицензия для использования **Dr.Web Shark** не требуется.

## Установка

**Dr.Web Shark** не требует установки. Вы можете начать работать с программой сразу же после завершения копирования исполняемого файла на компьютер, подлежащий проверке.

Для работы **Dr.Web Shark** требуется компьютер со следующей конфигурацией (табл. 2):



Таблица 2. Системные требования.


Компонент	Требование
Место на жестком диске	Не менее 3 МБ свободного пространства для исполняемого файла.
Операционная система	Microsoft® Windows® 2000 Server с пакетом обновлений 4 (SP4) или более поздняя версия.

Требования к остальным компонентам конфигурации совпадают с требованиями операционной системы.

## Запуск Dr.Web Shark

**Dr.Web Shark** может работать в одном из двух [режимов](#). Для начала работы в любом из режимов необходимо запустить приложение.

### Запуск Dr.Web Shark

1. Чтобы запустить **Dr.Web Shark** на выполнение, скопируйте исполняемый файл Dr.Web Shark в любую папку на компьютере, требующем проверки.
2. Дважды щелкните на значке **Dr.Web Shark** .

После запуска программы открывается окно [мастера Dr.Web Shark](#). Следуйте подсказкам мастера, чтобы начать работу с **Dr.Web Shark**.

## Мастер Dr.Web Shark

Окно мастера Dr.Web Shark открывается сразу же, как только вы запускаете **Dr.Web Shark**. С помощью мастера вы можете запустить консоль **Dr.Web Shark** или в фоновом режиме собрать данные для генерации отчета о работе операционной системы компьютера.



## Отображение консоли Dr.Web Shark

1. Чтобы отобразить консоль, запустите **Dr.Web Shark**. Откроется окно мастера Dr.Web Shark.
2. На шаге **Select operation mode page** выберите режим **Interactive mode**.
3. Нажмите кнопку **Finish**.



Прежде чем отобразить консоль **Dr.Web Shark** в фоновом режиме собирает данные о работе операционной системы. Сбор данных может занять некоторое время.


## Генерация отчета Dr.Web Shark

1. Чтобы создать отчет, запустите **Dr.Web Shark**. Откроется окно мастера Dr.Web Shark.
2. На шаге **Select operation mode** выберите режим **Report generation mode** и нажмите кнопку **Next**.
3. На шаге **Select tables to include to the report** выберите, какую информацию вы хотите поместить в отчет:
  - **Processes** - информация о процессах, выполняемых операционной системой;
  - **SSDT** - информация о записях в таблице системных вызовов System Service Descriptors Table;
  - **Drivers** - информация о драйверах, установленных в системе;
  - **Startups** - информация об объектах автозапуска.

Нажмите кнопку **Next**.

4. На шаге **Select path to save the report** выполните одно из следующих действий:
  - чтобы сохранить отчет в папке по умолчанию, введите название файла с отчетом;
  - чтобы сохранить отчет в любой другой папке, введите полный путь к файлу, в котором вы хотите сохранить отчет;



- чтобы открыть стандартный диалог Сохранить как, нажмите кнопку **Обзор**  и выберите, где сохранить отчет.

Нажмите кнопку **Next**.

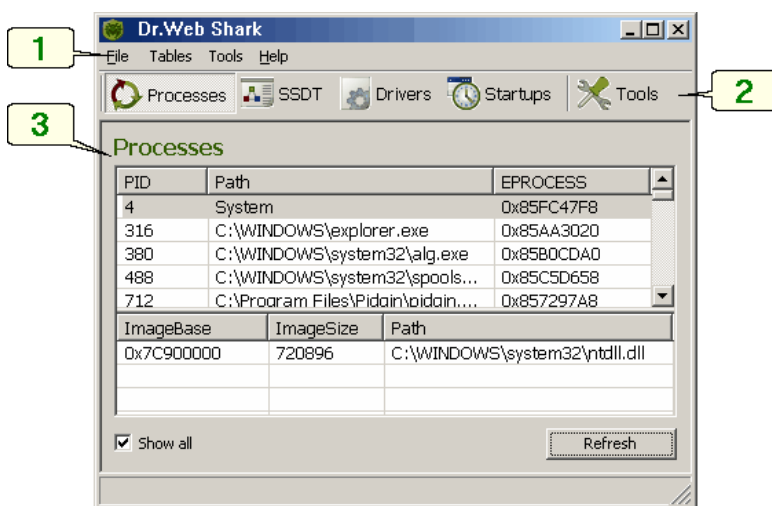
5. **Dr.Web Shark** собирает информацию о системе и формирует отчет. этот процесс может занять некоторое время. Чтобы отменить формирование отчета, нажмите кнопку **Cancel**.
6. Когда формирование отчета завершится, нажмите кнопку **Finish**.

Отчет сохраняется в указанной папке. По умолчанию используется папка, в которой находится исполняемый файл Dr.Web Shark.



## Глава 3. Консоль Dr.Web Shark

Консоль Dr.Web Shark представляет собой графический пользовательский интерфейс (GUI) для анализа и управления объектами операционной системы, изменение которых может свидетельствовать о присутствии на компьютере вредоносного программного обеспечения.



Легенда:

1. Меню.
2. Панель инструментов.
3. Вкладка отчета.

Окно консоли включает в себя:

- меню, которое предоставляет опции навигации и генерации отчета;
- панель инструментов, которая упрощает переключение между вкладками отчетов;



- [вкладки отчетов](#), которые отображают информацию о системе в режиме реального времени.

## Меню

Меню предоставляет вам доступ к следующей функциональности **Dr.Web Shark**:

Меню	Пункт меню	Комментарий
File	Save report	Отображает мастер Dr.Web Shark, с помощью которого вы можете собрать данные о системе и сформировать отчет Dr.Web Shark.
	Exit	Закрывает программу.
Tables	Processes	Открывает вкладку Processes.
	SSDT	Открывает вкладку SSDT.
	Drivers	Открывает вкладку Drivers.
	Startups	Открывает вкладку Startups.
	Tools	Открывает вкладку Tools.
Tools	Delete After Reboot...	Открывает диалог Delete After Reboot, в котором вы можете пометить любой файл для удаления после следующей перезагрузки компьютера.
Help	Online Help	Отображает Справку по программе.
	About...	Отображает информацию о программе.

## Панель инструментов

Панель инструментов позволяет вам быстро переключаться между [вкладками отчетов](#).



## Вкладки отчетов

Вкладки отчетов в режиме реального времени отображают информацию о настройках и объектах операционной системы. Динамический отчет разделен на следующие вкладки:

- вкладка **Processes**, отображающая информацию о процессах, выполняемых операционной системой;
- вкладка **SSDT**, отображающая информацию о записях в таблице системных вызовов System Service Descriptors Table;
- вкладка **Drivers**, отображающая информацию о драйверах, установленных в системе;
- вкладка **Startups**, отображающая информацию об объектах автозапуска.

Также на вкладке **Tools** вы можете воспользоваться дополнительными инструментами, отображающими информацию о файловой системе и загрузочных записях дисков (MBR).

### Вкладка Processes

На этой вкладке отображаются сведения о процессах, запущенных на компьютере, и модулях, которые процессы используют.

Большинство стандартных средств, таких как Диспетчер Задач операционной системы Microsoft Windows, используют для сбора данных высокоуровневые функции. Некоторые вредоносные программы способны встраиваться на промежуточные уровни операционной системы и подменять результаты, возвращаемые высокоуровневыми функциями. **Dr.Web Shark**, в дополнение к стандартным методам, использует также низкоуровневую технологию **Dr.Web Shield**, которая позволяет собирать достоверную информацию даже о тех процессах, которые вредоносные программы скрывают или незаконно используют. Например, вирус может присвоить своему процессу идентификатор (PID), который уже использует другой процесс. Это позволяет вирусу скрыться от пользователей, использующих





стандартные утилиты, которые отображают только один процесс для каждого идентификатора.

**Dr.Web Shark** обнаруживает расхождения в результатах, полученных с использованием разных функций, и выделяет цветом подозрительные процессы:

Цвет	Комментарий
Красный	Указывает на скрытый процесс или модуль.
Желтый	Указывает на процесс, использующий один или более скрытых модулей.

### Представление результатов

Чтобы изменить представление, выполните одно из следующих действий:

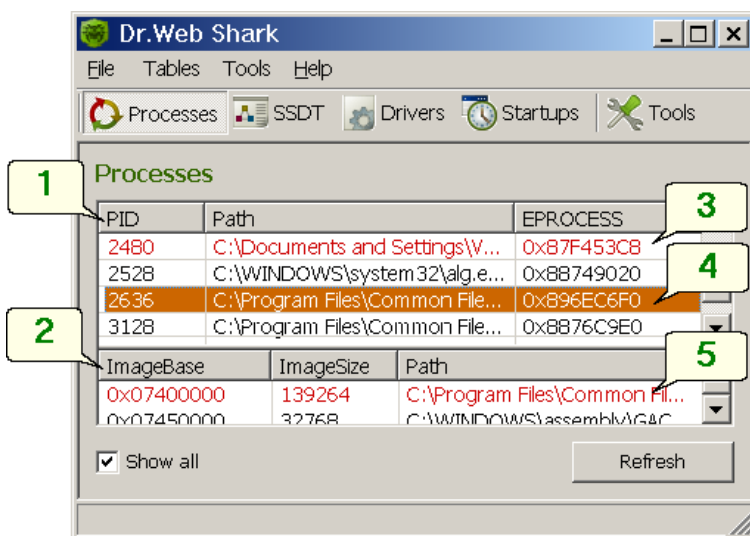
- чтобы отобразить в списке только подозрительные процессы, снимите флажок **Show All**;
- чтобы отобразить в списке все процессы, установите флажок **Show All**.

### Обновление

Чтобы обновить информацию в списке, нажмите кнопку **Refresh**.

На этой вкладке вы можете прервать подозрительный процесс или создать дампы памяти модулей, которые он использует. Эти методы помогут вам прекратить выполнение вредоносной программы и собрать данные для анализа.

Более подробно процедуры описаны в разделе [Управление процессами](#).



Легенда:

1. Панель процессов.
2. Панель модулей.
3. Скрытый процесс.
4. Процесс, использующий скрытые модули.
5. Скрытый модуль.

## Вкладка SSDT

На этой вкладке отображаются сведения о функциях, выполняющихся в режиме ядра.

Пользовательские приложения обращаются к таким функциям, чтобы получить доступ к функциональности ядра операционной системы. Указатели на функции хранятся в таблице системных вызовов System Service Descriptor Table (SSDT). Часто вредоносные программы пытаются изменить указатели так, чтобы при вызове стандартной функции управление передалось на вредоносный код. Поскольку для сбора информации о системе чаще всего



используются именно системные функции из таблицы SSDT, то их "перехват" (изменение указателей в таблице системных вызовов) позволяет вредоносным программам скрываться от стандартных утилит.

**Dr.Web Shark** обнаруживает и выделяет цветом перехваченные или незаконно добавленные в таблицу системные функции.

### Представление результатов

Чтобы изменить представление, выполните одно из следующих действий:

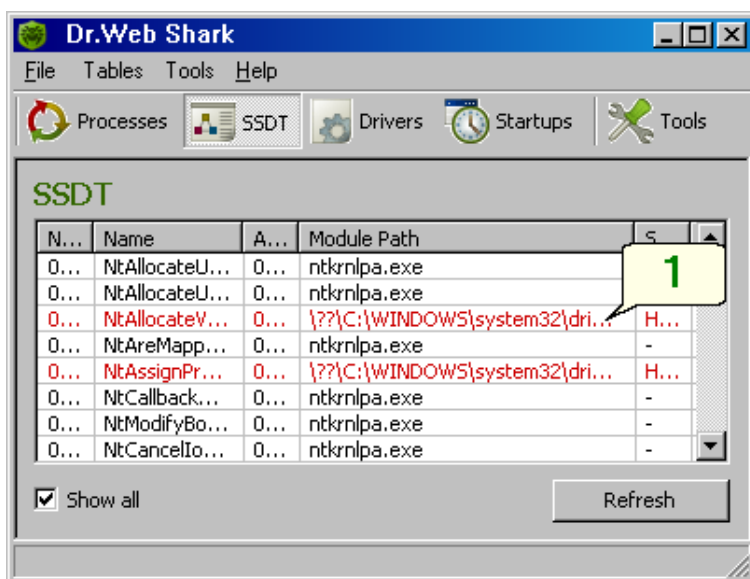
- чтобы отобразить в списке только перехваченные функции, снимите флажок **Show All**;
- чтобы отобразить в списке все функции, установите флажок **Show All**.

### Обновление

Чтобы обновить информацию в списке, нажмите кнопку **Refresh**.

На этой вкладке вы можете нейтрализовать последствия работы вредоносных программ путем восстановления правильных указателей на системные функции ("снятия перехвата").

Более подробно процедуры описаны в разделе [Управление системными сервисами](#).



Легенда:

1. Перехваченная функция.

## Вкладка Drivers

На этой вкладке отображаются сведения о драйверах, установленных на компьютере.

Драйвера выполняются в режиме ядра, так как для работы с оборудованием им нужен доступ к низкоуровневым функциям и объектам операционной системы. Некоторые вирусы пользуются этой особенностью, чтобы получить доступ к ресурсам ядра.

**Dr.Web Shark** обнаруживает и выделяет цветом все драйвера, скрытые от стандартных утилит операционной системы, а так же те драйвера, которые ссылаются на несуществующие файлы драйверов.



## Представление результатов

Чтобы изменить представление, выполните одно из следующих действий:

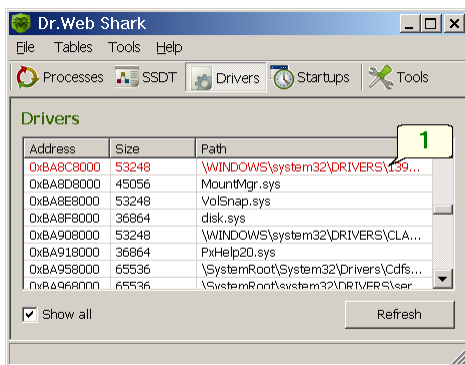
- чтобы отобразить в списке только подозрительные драйвера, снимите флажок **Show All**;
- чтобы отобразить в списке все драйвера, установите флажок **Show All**.

## Обновление

Чтобы обновить информацию в списке, нажмите кнопку **Refresh**.

На этой вкладке вы можете создать дамп памяти драйвера или произвольной области памяти ядра. Эти методы помогут вам собрать данные для анализа, в том числе получить информацию из дополнительных областей памяти ядра, если она необходима.

Более подробно процедуры описаны в разделе [Управление драйверами](#).



Легенда:

1. Подозрительный драйвер.



## Вкладка Startups



Данные для этой вкладки собираются только по запросу пользователя. чтобы собрать данные об объектах автозапуска, нажмите кнопку **Refresh**.

На этой вкладке отображаются сведения об объектах, автоматически загружаемых в память при запуске системы.

Данные для этого отчета собираются из реестра операционной системы. Некоторые вредоносные программы могут "перехватывать" системные функции, выполняющие сбор данных для таких стандартных утилит, как Редактор реестра операционной системы Microsoft Windows. Это позволяет вредоносным программам прятать данные реестра или модифицировать информацию, которую стандартные утилиты предоставляют пользователю.

**Dr.Web Shark** использует функции непосредственного чтения памяти (raw read) для сбора данных реестра. Этот метод позволяет обнаруживать несоответствия в результатах, полученных с использованием стандартных функций и низкоуровневых технологий.

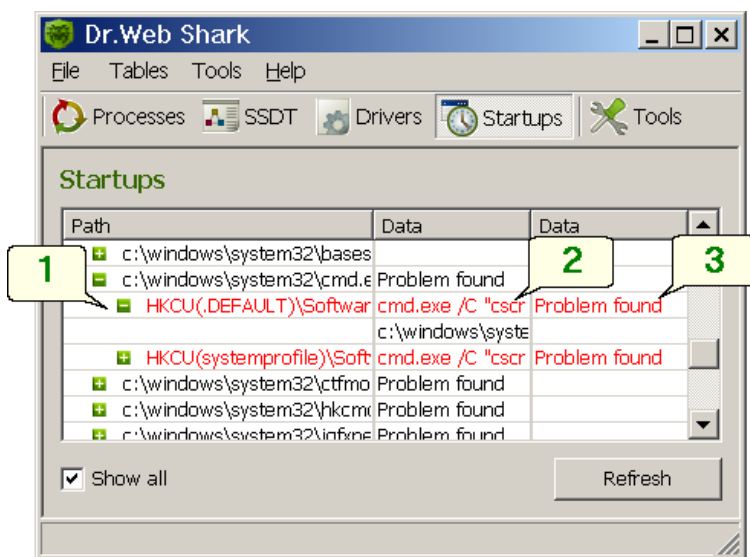
### Представление результатов

Чтобы изменить представление, выполните одно из следующих действий:

- чтобы отобразить в списке только подозрительные объекты автозапуска, снимите флажок **Show All**;
- чтобы отобразить в списке все объекты автозапуска, установите флажок **Show All**.

### Обновление

Чтобы обновить информацию в списке, нажмите кнопку **Refresh**.



Легенда:

1. Объект автозапуска.
2. Значение параметра.
3. Комментарий о несоответствии результатов.

## Дополнительные инструменты

На этой вкладке вы можете воспользоваться дополнительными инструментами для сбора информации о системе.

Вы можете использовать следующие инструменты:

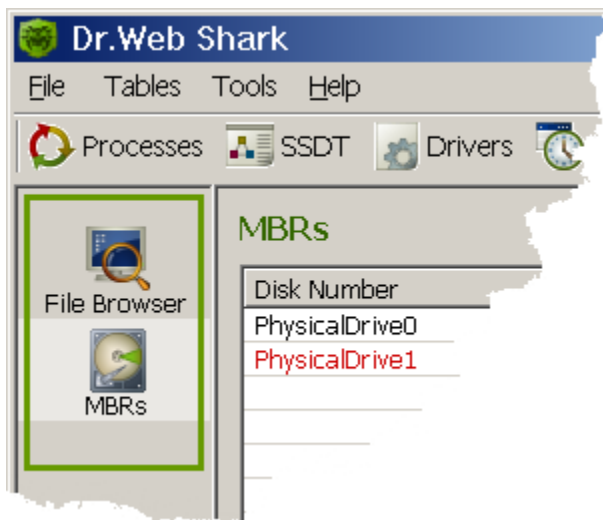
- [File Browser](#)
- [Master Boot Records \(MBRs\) Browser](#)

### Переключение между инструментами

Чтобы переключиться на использование другого инструмента,



нажмите на значок нужного инструмента на панели:



## Инструмент File Browser

Инструмент File Browser отображает содержимое локальной файловой системы.

Большинство стандартных средств, таких как Проводник операционной системы Microsoft Windows, используют для просмотра файловой системы высокоуровневые функции. Некоторые вредоносные программы способны встраиваться на промежуточные уровни операционной системы и подменять результаты, возвращаемые высокоуровневыми функциями.

Dr.Web Shark File Browser использует низкоуровневую технологию **Dr.Web Shield**, которая позволяет отображать и управлять всеми объектами файловой системы и в том числе теми, которые вредоносные программы скрывают или блокируют.

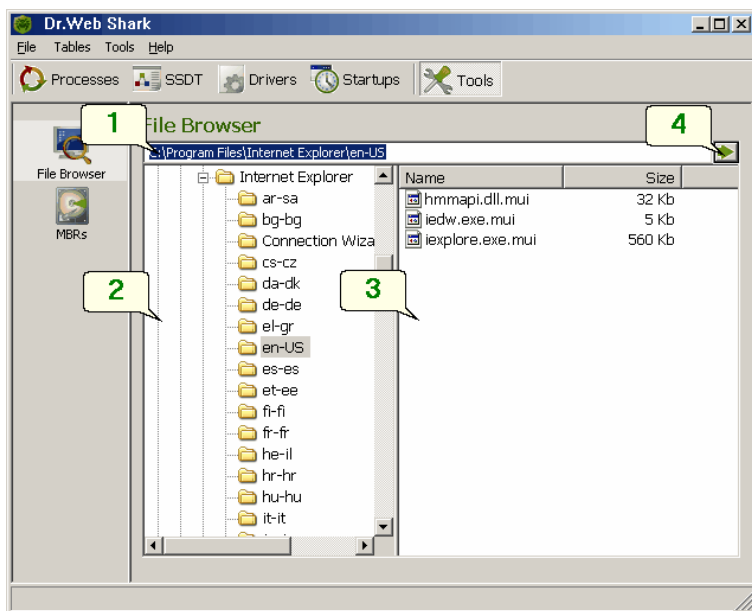
С помощью этого инструмента вы можете копировать файлы, упаковывать подозрительные файлы для анализа, так же удалять





файлы или пометить для удаления после перезагрузки системы. Эти методы помогут вам удалить вредоносные программы и подготовить подозрительные файлы для анализа.

Более подробно процедуры описаны в разделе [Управление файлами](#).



Легенда:

1. Адресная строка.
2. Навигационная панель.
3. Панель выбора файла.
4. Кнопка перехода.

## Инструмент MBRs Browser

Инструмент MBRs Browser отображает загрузочные записи дисков,



разбитых на логические разделы.

Некоторые вредоносные программы могут блокировать доступ к загрузочным записям или "[перехватывать](#)" системные функции, что позволяет им модифицировать информацию, которую стандартные утилиты предоставляют пользователю (например, представлять измененные записи правильными).

Dr.Web Shark MBRs Browser использует низкоуровневую технологию **Dr.Web Shied**, что позволяет обнаруживать несоответствия в результатах, полученных с использованием стандартных функций и специальных технологий.

### Представление результатов

Чтобы изменить представление, выполните одно из следующих действий:

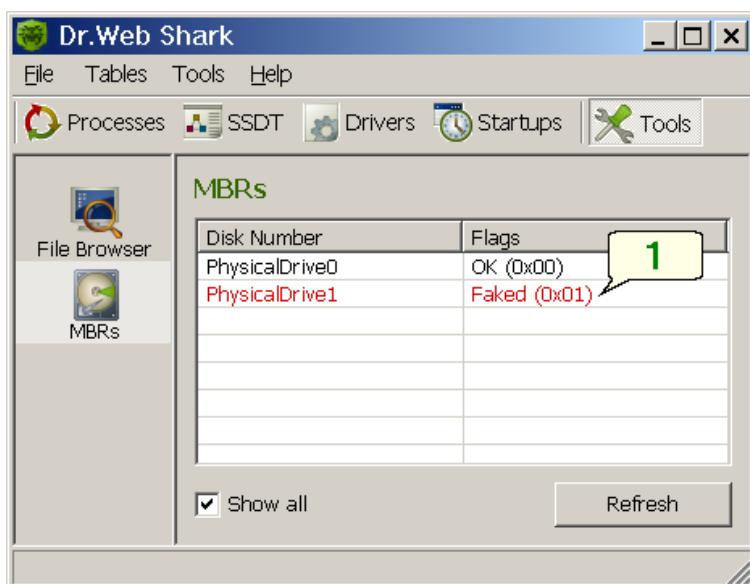
- чтобы отобразить в списке только измененные или недоступные загрузочные записи, снимите флажок **Show All**;
- чтобы отобразить в списке все загрузочные записи, установите флажок **Show All**.

### Обновление

Чтобы обновить информацию в списке, нажмите кнопку **Refresh**.

С помощью этого инструмента вы также можете создавать дампы загрузочных записей для анализа.

Более подробно процедуры описаны в разделе [Создание дампов памяти](#).



Легенда:

1. Недоступная или измененная загрузочная запись.



## Глава 4. Нейтрализация угроз

Этот раздел описывает как нейтрализовать угрозы, обнаруженные с помощью **Dr.Web Shark**.

Вы можете:

- [управлять процессами](#);
- [управлять системными сервисами](#);
- [управлять драйверами](#);
- [управлять файлами](#);
- [создавать дампы памяти](#).

### Управление процессами

Для управления системными процессами используется вкладка [Processes](#).

Вы можете:

- [прервать процесс](#);
- [создать дамп](#) модуля, используемого процессом;
- [изменить представление](#) результатов;
- [обновить информацию](#).



Прерывание некоторых процессов может нарушить стабильность работы операционной системы вплоть до возникновения критических системных ошибок (BSOD).

### Прерывание процессов

1. Чтобы прервать процесс, выберите его в панели процессов.
2. В контекстном меню процесса выберите **Kill process**.



Завершение процесса может потребовать некоторого времени. Дождитесь сообщения о завершении в строке состояния.

### Создания дампа модуля

1. Чтобы создать дамп модуля, используемого процессом, в панели процессов выберите интересующий процесс.
2. В панели модулей выберите интересующий модуль.
3. В контекстном меню модуля выберите **Dump module**.
4. В стандартном диалоге **Сохранить как** выберите, где вы хотите сохранить дамп, и нажмите кнопку **Save**.

### Представление результатов

Чтобы изменить представление, выполните одно из следующих действий:

- чтобы отобразить в списке только подозрительные процессы, снимите флажок **Show All**;
- чтобы отобразить в списке все процессы, установите флажок **Show All**.

### Обновление

Чтобы обновить информацию в списке, нажмите кнопку **Refresh**.

## Управление системными сервисами

Для "снятия перехвата" с системных сервисов используется вкладка [SSDT](#).

Вы можете:

- [снять перехват с функции](#);
- [снять перехват со всех функций](#);
- [изменить представление](#);
- [обновить информацию](#).



Изменение указателей на системные функции (снятие перехвата) может нарушить стабильность работы операционной системы вплоть до возникновения критических системных ошибок (BSOD).

### Снятие перехвата с функции

1. Чтобы снять перехват с конкретной функции, выберите функцию в списке.
2. В контекстном меню функции выберите **Unhook**.

Восстановление указателя функции может занять некоторое время. Дождитесь сообщения о завершении в строке состояния.

### Снятие всех перехватов

1. Чтобы снять перехваты со всех системных функций, выберите любую функцию в списке.
2. В контекстном меню функции выберите **Unhook All**.

Восстановление указателей функций может занять некоторое время. Дождитесь сообщения о завершении в строке состояния..

### Представление результатов

Чтобы изменить представление, выполните одно из следующих действий:

- чтобы отобразить в списке только перехваченные функции, снимите флажок **Show All**;
- чтобы отобразить в списке все функции, установите флажок **Show All**.

### Обновление

Чтобы обновить информацию в списке, нажмите кнопку **Refresh**.



## Управление драйверами

Для управления установленными драйверами используется вкладка [Drivers](#).

Вы можете:

- [создать дамп драйвера](#);
- [создать дамп](#) произвольной области памяти ядра;
- [изменить представление](#);
- [обновить информацию](#).

### Создания дампа драйвера

1. Чтобы создать дамп памяти драйвера, выберите интересующий драйвер в списке.
2. В контекстном меню драйвера выберите **Dump driver**.
3. В стандартном диалоге Сохранить как выберите, где вы хотите сохранить дамп, и нажмите кнопку **Save**.

### Создание дампа произвольной области памяти ядра

1. Чтобы создать дамп произвольной области памяти, выберите интересующий драйвер в списке.
2. В контекстном меню драйвера выберите **Dump memory**.
3. В диалоге **Dump Memory** выберите базовый адрес и размер сегмента памяти, для которого вы хотите создать дамп. Нажмите кнопку **Save As**.



По умолчанию, параметрам **Base address** и **Size** присваиваются значения, определяющие пространство драйвера в памяти ядра.

---

4. В стандартном диалоге **Сохранить как** выберите, где вы хотите сохранить дамп, и нажмите кнопку **Save**.



## Представление результатов

Чтобы изменить представление, выполните одно из следующих действий:

- чтобы отобразить в списке только подозрительные драйвера, снимите флажок **Show All**;
- чтобы отобразить в списке все драйвера, установите флажок **Show All**.

## Обновление

Чтобы обновить информацию в списке, нажмите кнопку **Refresh**.

## Управление файлами

Для управления файлами используется вкладка [File Browser](#).

Вы можете:


- [копировать](#) файлы с использованием низкоуровневых функций, если вредоносные программы блокируют копирование;
- [упаковывать подозрительные файлы](#) в специальный архивы, включающие подозрительный файл и всю необходимую для анализа информацию;
- [удалять](#) файлы с использованием низкоуровневых функций, если вредоносные программы блокируют удаление;
- помечать файлы для [удаления после перезагрузки](#) системы, если подозрительный файл в данный момент используется.

## Копирование файлов

1. Чтобы копировать файл, выберите его. Для этого выполните одно из следующих действий:
  - используйте навигационную панель, чтобы выбрать папку, в которой хранится файл, а затем выберите файл в панели выбора файлов;





- введите полный путь к файлу в у адресной строке и нажмите кнопку **Перейти** .
2. В контекстном меню файла выберите **Сору**.
  3. В стандартном диалоге **Сохранить как** выберите, куда вы хотите копировать файл, и нажмите кнопку **Save**.


### Упаковка подозрительных файлов для анализа

1. Чтобы упаковать подозрительный файл и всю необходимую для анализа информацию, выберите файл. Для этого выполните одно из следующих действий:
  - используйте навигационную панель, чтобы выбрать папку, в которой хранится файл, а затем выберите файл в панели выбора файлов;
  - введите полный путь к файлу в у адресной строке и нажмите кнопку **Перейти** .
2. В контекстном меню файла выберите **Quarantine**.
3. В диалоге **Browse for Folder** выберите, где вы хотите сохранить пакет, и нажмите кнопку **OK**.



При подготовке пакета **Dr.Web Shark** не удаляет подозрительный файл. Пакет включает в себя копию подозрительного файла и общую информацию о системе, необходимую для проведения анализа.

### Удаление файлов


1. Чтобы удалить файл, выберите его. Для этого выполните одно из следующих действий:
  - используйте навигационную панель, чтобы выбрать папку, в которой хранится файл, а затем выберите файл в панели выбора файлов;
  - введите полный путь к файлу в у адресной строке и нажмите кнопку **Перейти** .
2. В контекстном меню файла выберите **Delete**.



3. **Dr.Web Shark** запросит подтверждение действия. Нажмите кнопку **Yes**.

**Dr.Web Shark** удаляет выбранный файл.

### Удаление файлов после перезагрузки

1. Чтобы пометить файл для удаления после перезагрузки системы, выберите его. Для этого выполните одно из следующих действий:
  - используйте навигационную панель, чтобы выбрать папку, в которой хранится файл, а затем выберите файл в панели выбора файлов;
  - введите полный путь к файлу в у адресной строке и нажмите кнопку **Перейти** .
2. В контекстном меню файла выберите **Delete after reboot**.
3. **Dr.Web Shark** запросит подтверждение действия. Нажмите кнопку **Yes**.
4. Файл будет удален после следующей перезагрузки системы. **Dr.Web Shark** предложит вам провести перезагрузку немедленно. Чтобы перезагрузить систему, нажмите кнопку **Yes** (рекомендуется). Чтобы отложить перезагрузку, нажмите кнопку **No**.



---

Диалог **Delete After Reboot** доступен на любой вкладке. Чтобы открыть диалог, в меню выберите **Tools -> Delete After Reboot**. Эта опция помогает пометить на удаление подозрительный файлы, выделенные **Dr.Web Shark** на других [вкладках отчетов](#).

---

## Создание дампов памяти

С помощью **Dr.Web Shark** вы можете создавать дампы памяти для сбора информации о подозрительных объектах операционной системы.



Вы можете создавать дампы следующих объектов:

- [модулей](#), используемых процессами;
- [загрузочных записей](#);
- [драйверов](#);
- [произвольных областей](#) памяти ядра.

### Создание дампа модуля процесса

1. Чтобы создать дамп модуля, выберите вкладку [Processes](#).
2. В панели процессов выберите интересующий процесс.
3. В панели модулей выберите интересующий модуль.
4. В контекстном меню модуля выберите **Dump module**.
5. В стандартном диалоге **Сохранить как** выберите, где вы хотите сохранить дамп, и нажмите кнопку **Save**.

### Создание дампа загрузочной записи

1. Чтобы создать дамп загрузочной записи, выберите вкладку [Tools](#).
2. Выберите инструмент MBRs.
3. В списке загрузочных записей выберите интересующую запись.
4. В контекстном меню записи выберите **Dump MBR**.
5. В стандартном диалоге **Сохранить как** выберите, где вы хотите сохранить дамп, и нажмите кнопку **Save**.

### Создание дампа драйвера

1. Чтобы создать дамп памяти драйвера, выберите вкладку [Drivers](#).
2. Выберите интересующий драйвер в списке.
3. В контекстном меню драйвера выберите **Dump driver**.
4. В стандартном диалоге **Сохранить как** выберите, где вы хотите сохранить дамп, и нажмите кнопку **Save**.

### Создание дампа произвольной области памяти ядра

1. Чтобы создать дамп произвольной области памяти, выберите вкладку [Drivers](#).



2. Выберите интересующий драйвер в списке.
3. В контекстном меню драйвера выберите **Dump memory**.
4. В диалоге **Dump Memory** выберите базовый адрес и размер сегмента памяти, для которого вы хотите создать дамп. Нажмите кнопку **Save As**.



По умолчанию, параметрам **Base address** и **Size** присваиваются значения, определяющие пространство драйвера в памяти ядра.

---

5. В стандартном диалоге **Сохранить как** выберите, где вы хотите сохранить дамп, и нажмите кнопку **Save**.



## Глава 6. Генерация отчетов

Функция формирования отчетов Dr.Web Shark позволяет вам собирать информацию о системе с использованием низкоуровневой технологии **Dr.Web Shield** и сохранять полученные данные в формате XML. Отчеты Dr.Web Shark могут использоваться в качестве снимков состояния системы для аудита, или предоставляться для анализа и обнаружения вредоносных программ специалистам [службы технической поддержки](#) ООО «Доктор Веб».

Отчеты включают информацию о следующих системных объектах:

- процессах, запущенных в системе;
- записях таблицы системных вызовов System Service Descriptors Table;
- драйверах, установленных в системе;
- объектах автозапуска.

Отчеты могут формироваться как из консоли, так и напрямую из мастера Dr.Web Shark.


### Генерация отчета Dr.Web Shark

1. Чтобы создать отчет, воспользуйтесь одним из следующих способов, чтобы открыть мастер Dr.Web Shark на шаге **Select tables to include to the report**:
  - чтобы сформировать отчет без запуска консоли, [запустите](#) Dr.Web Shark в режиме [генерации отчета](#).
  - чтобы сформировать отчет из консоли, выберите в меню **File -> Save Report**.
2. На шаге **Select tables to include to the report** выберите, какую информацию вы хотите поместить в отчет:
  - **Processes** - информация о процессах, выполняемых операционной системой;
  - **SSDT** - информация о записях в таблице системных вызовов System Service Descriptors Table;



- **Drivers** - информация о драйверах, установленных в системе;
- **Startups** - информация об объектах автозапуска.

Нажмите кнопку **Next**.

3. На шаге **Select path to save the report** выполните одно из следующих действий:
  - чтобы сохранить отчет в папке по умолчанию, введите название файла с отчетом;
  - чтобы сохранить отчет в любой другой папке, введите полный путь к файлу, в котором вы хотите сохранить отчет;
  - чтобы открыть стандартный диалог Сохранить как, нажмите кнопку **Обзор**  и выберите, где сохранить отчет.

Нажмите кнопку **Next**.

5. **Dr.Web Shark** собирает информацию о системе и формирует отчет. Этот процесс может занять некоторое время. Чтобы отменить формирование отчета, нажмите кнопку **Cancel**.
6. Когда формирование отчета завершится, нажмите кнопку **Finish**.

Отчет сохраняется в указанной папке. По умолчанию используется папка, в которой находится исполняемый файл Dr.Web Shark.

---

