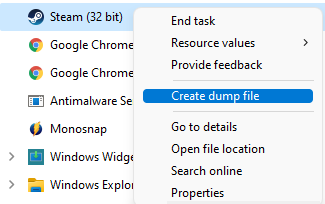
Дампы нужны что бы приатачить их к дефекту

Можно использовать программу **Windbg** или команду CMD **procdump** или **диспетчер задач**

Что бы снять дампы процесса, **используем диспетчер задач**



Или утилиту командной строки **procdump** (нужно скачать заранее)

Основная цель ProcDump — следить за приложениями, чтобы они не перегружали центральный процессор и не создавали аварийные ситуации. В случае аварийной ситуации утилита ProcDump создаст дамп, чтобы пользователь смог выяснить, из-за чего случилась авария. Утилита может:

* отследить работу системных и пользовательских приложений;
* отследить причину зависания окна «Проводника»;
* мониторить необработанные исключения;
* создавать дампы, основываясь на счетчиках производительности системы;
* быть встроенной в пользовательские скрипты;
* и др.

**Как пользоваться procdump**

1. Необходимо на диске С создать папку с именем «ProcDump», куда будут записываться дамп-файлы с расширением «.dmp» о контролируемых процессах.
2. Открыть консоль и написать команду захвата процесса. Команда составляется по следующему шаблону: «**procdump.exe [ обозначение процесса] {программа, процесс или файл, который нужно будет контролировать}**». Например: «procdump.exe -ma -e -mp worldoftanks.exe», где «worldoftanks.exe» — это файл, который нужно отследить, а «-ma -e -mp» — это параметры, которые нужно отследить.
3. Проверить папку «ProcDump» на наличие записанных дампов.

**Примеры параметров для ProcDump**

Приведем примеры основных параметров для отслеживания, которые применяются в утилите ProcDump:

* «-а» — избегать перебоев в работе;
* «-at» — избегать простоев после окончания времени ожидания;
* «-b» — рассматривать точки останова отладки как исключение;
* «-с» — верхний уровень нагрузки центрального процессора, при котором активируется дамп процесса;
* «cl» — нижний уровень нагрузки центрального процессора, при котором активируется дамп процесса;
* «-е» — записать дамп, когда обнаружится необработанное исключение;
* «-f» — указывает фильтр исключения для записи первого дампа;
* «-fx» — указывает фильтр исключения для записи всех дампов в журнал;
* «-g» — запуск собственного отладчика процессов;
* «-h» — запись дампа при зависании окон;
* «-i» — запускает ProcDump как последнюю инстанцию дебага;
* «-k» — завершает процесс клонирования (-r) и запись дампов;
* «-l» — презентовать журнал отладки процесса;
* «-m» — порог использования памяти в Мб, при котором создается дамп;
* «-mа» — записать дамп при указанном объеме используемой памяти;
* «-mk» — записать дамп памяти ядра операционной системы;
* «-ml» — записать дамп, когда объем памяти упадет ниже указанного значения;
* «-mm» — записать мини-дамп;
* «-mp» — запись подробного дампа со всей информацией о потоках и используемой памяти;
* «-n» — указывается количество дампов, после которых ProcDump завершает работу;
* «-о» — перезапись существующего дампа;
* «-p» — запись дампа при превышении указанного порога производительности системы;
* «-pl» — запись дампа, когда уровень производительности упадет ниже указанного порога;
* «-r» — запись дампа у клона системы;
* «-s» — указать секунды перед записью дампа;
* «-t» — запись дампа после окончания процесса;
* «-u» — рассматривать нагрузку на одно ядро центрального процессора;
* «-w» — ждать запуска указанного процесса;
* «wer» — самый большой дамп записать последним в очереди;
* «-64» — создание 64-битного дампа, по умолчанию ProcDump создает 32-битный дамп.
* И др.

**Примеры использования ProcDump**

Приведем несколько примеров использования утилиты ProcDump:

* записать мини-дамп приложения «Блокнот» — **procdump notepad**;
* записать 4 мини-дампа приложения «Блокнот» с интервалом в 6 секунд — **procdump -s 6 -n 4 notepad**;
* записать 2 мини-дампа процесса «производительность» с интервалом 6 секунд, когда нагрузка на центральный процессор превысит 25% — **procdump -c 25 -s 6 -n 2 consume**;
* записать мини-дамп процесса с именем «example.exe», когда его окно зависает более чем на 5 секунд — **procdump -h example.exe examplewindows.dmp**;
* и др.

1. Откройте **редактор реестра.**

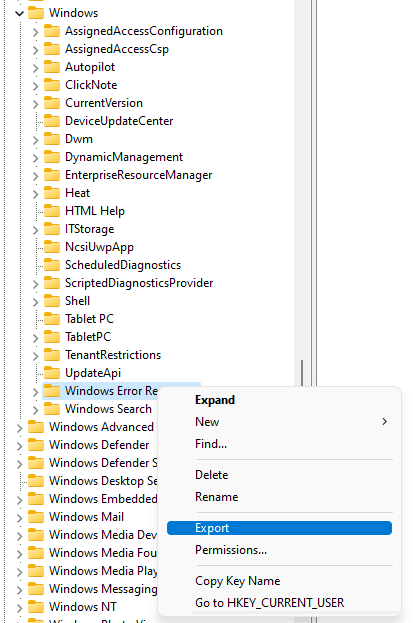
Выполните следующие действия, чтобы открыть **редактор реестра**:

* 1. Нажмите **Win + R**, чтобы открыть окно команды **Выполнить**.
  2. Введите **regedit** в окно **Выполнить** и нажмите клавишу «Ввод».
  3. Нажмите **Да** во всплывающем окне **Управление пользователями**.

1. Создайте резервную копию раздела **Windows Error Reporting.**

Перед внесением каких-либо изменений в **редакторе реестра** рекомендуется создать резервную копию раздела реестра, который вы собираетесь редактировать. Ниже приведены инструкции по созданию резервной копии:

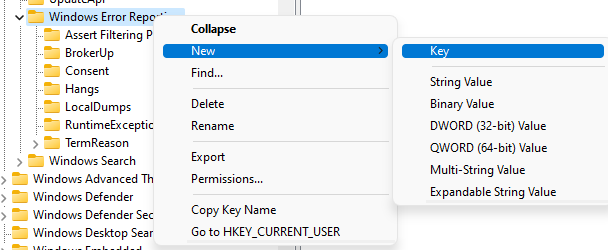
* 1. Перейдите в расположение **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\**.
  2. Щелкните правой кнопкой мыши раздел **Windows Error Reporting**.
  3. Выберите **Экспортировать** и сохраните файл **.**reg на рабочем столе.



1. Создайте раздел **LocalDumps**.

Выполните следующие действия:

* 1. Перейдите в расположение: **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting**.
  2. Выберите раздел **Windows Error Reporting** и создайте новый раздел с именем **LocalDumps**, если его там еще нет:
     1. Щелкните правой кнопкой мыши **Windows Error Reporting.**
     2. Выберите **Создать**, а затем **Раздел.**
     3. Назовите раздел **LocalDumps.**



**Примечание.**

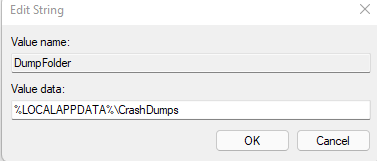
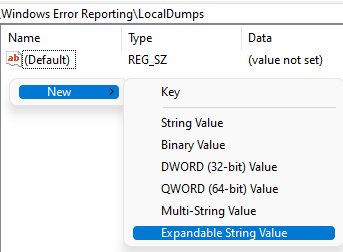
Убедитесь, что вы создали резервную копию раздела **Windows Error Reporting** перед созданием нового раздела.

1. Создайте значения реестра в разделе **LocalDumps.**

Выберите раздел **LocalDump** и создайте три значения реестра, указанные ниже:

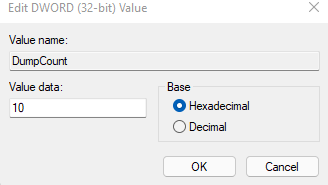
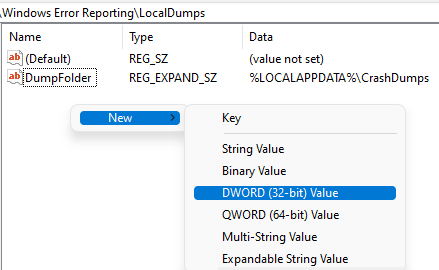
**Значение реестра DumpFolder**

* Щелкните правой кнопкой мыши на пустом месте в правой части и выберите **Создать**> **Расширяемый строковый параметр**
* Назовите его **DumpFolder**
* Дважды щелкните по нему и введите **%LOCALAPPDATA%\CrashDumps** в поле **Значение**.



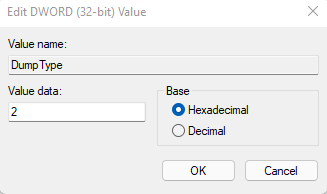
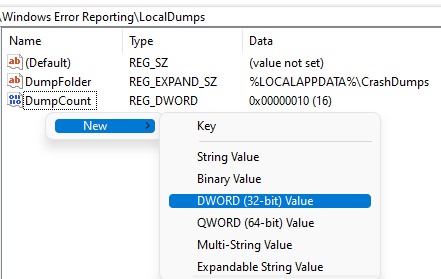
**Значение реестра DumpCount**

* Щелкните правой кнопкой мыши на пустом месте в правой части и выберите **Создать**> **Параметр DWORD (32 бита)**.
* Назовите его **DumpCount**
* Дважды щелкните по нему и введите **10** в поле **Значение**.



**Значение реестра DumpType**

* Щелкните правой кнопкой мыши на пустом месте в правой части и выберите **Создать**> **Параметр DWORD (32 бита)**.
* Назовите его **DumpType**
* Дважды щелкните по нему и введите **2** в поле **Значение**.



**Сбор аварийных дампов**

После выполнения инструкций в разделе [Включение аварийных дампов](https://helpx.adobe.com/ru/xd/kb/how-to-generate-crash-dump-on-windows-machine.html#EnablCrashDumps) воспроизведите сбой программного обеспечения и найдите соответствующий файл .dmp с названием программного обеспечения в папке **%localAppdata%\Packages\Adobe.CC.XD\_adky2gkssdxte\AC\Dumps**.

Чтобы сделать это, можно запустить команду **Пуск > Выполнить > %localAppdata%\Packages\Adobe.CC.XD\_adky2gkssdxte\AC\Dumps.**