

Лабораторная работа. Сравнение данных с помощью хэш-функции

Задачи

Использовать программу хэширования для проверки целостности данных.

Исходные данные/сценарий

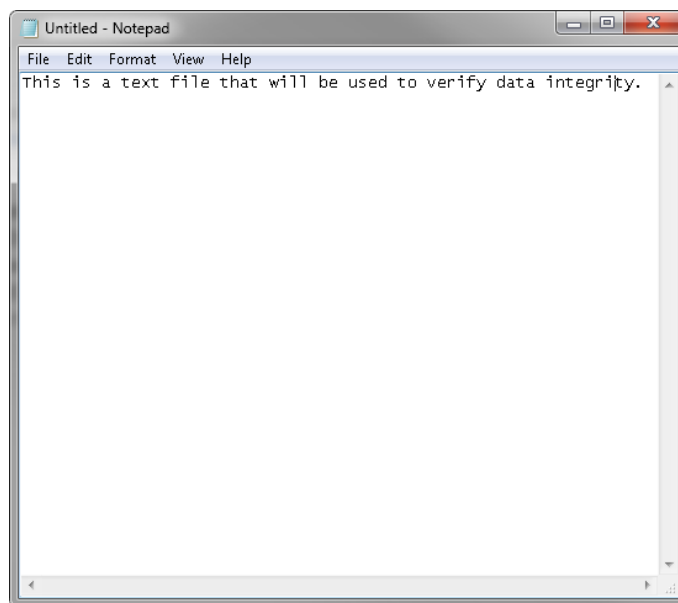
Важно понимать, были ли данные повреждены или была совершена попытка их фальсификации. Для определения того, были ли данные изменены или остались такими же, можно использовать программу хэширования. Программа хэширования выполняет преобразование данных или файла используя хэш-функцию, которая выдает некое значение (обычно значительно короче, чем сами исходные данные). Существует множество разных хэш-функций, одни очень простые, другие, напротив, очень сложные. Если одна и та же хэш-функция выполняется для преобразования одних и тех же данных, то значение, которое будет получено, будет всегда одинаково. Если данные были каким-то образом изменены, то полученное значение хэш-функцией будет отличаться.

Необходимые ресурсы

- ПК с доступом в Интернет

Шаг 1: Создайте текстовый файл

- Найдите на своем компьютере программу Notepad и откройте ее.
- Введите текст в программу.



- Выберите **File > Save (Файл > Сохранить)**.
- Перейдите на **Desktop (Рабочий стол)**.
- Введите **Hash** в поле **File name: (Имя файла:)** и нажмите **Save (Сохранить)**.

Шаг 2: Установите HashCalc

- а. Откройте веб-браузер и перейдите по ссылке: <http://www.slavasoft.com/download.htm>.

The screenshot shows the SlavaSoft website with a navigation menu on the left and a main content area. The main content area is titled "SlavaSoft Downloads" and features two sections: "FREE TRIAL SOFTWARE DOWNLOADS" and "FREE SOFTWARE DOWNLOADS".

SlavaSoft Downloads

FREE TRIAL SOFTWARE DOWNLOADS

You can download fully functional evaluation versions of our products and **try them for free**. This is so you will get a good feel about how the software works and how you can benefit from it. An **evaluation** version may be converted into a **registered** version by entering a valid [registration code](#). Please refer to the products' help files for detailed information about registration.

Product Name and Version	Operating System	Size	Free Trial Limitation	Download
Paint Express 1.31	Windows 95/98/Me/NT/2000/XP	1.71MB	60 uses	Download
QuickHash Library 3.02	Windows 95/98/Me/NT/2000/XP	692KB	10-second delay	Download
FastCRC Library 1.51	Windows 95/98/Me/NT/2000/XP	272KB	10-second delay	Download

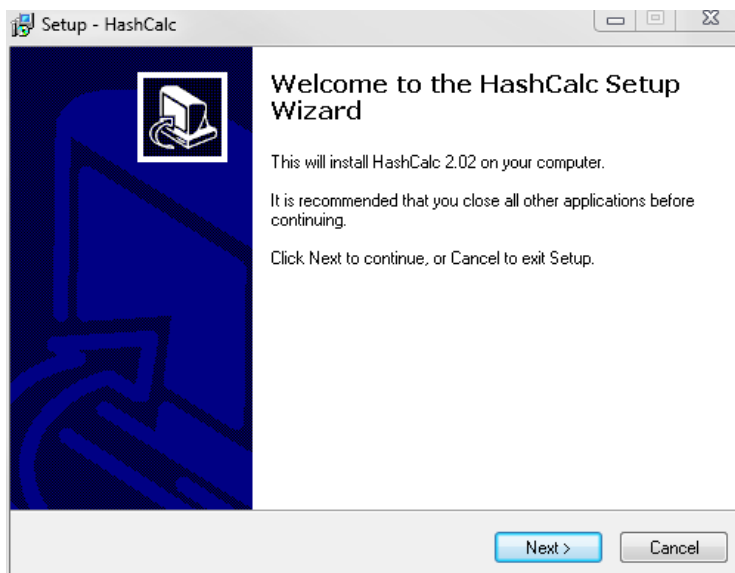
FREE SOFTWARE DOWNLOADS

You can download the following products and **use them for free**.

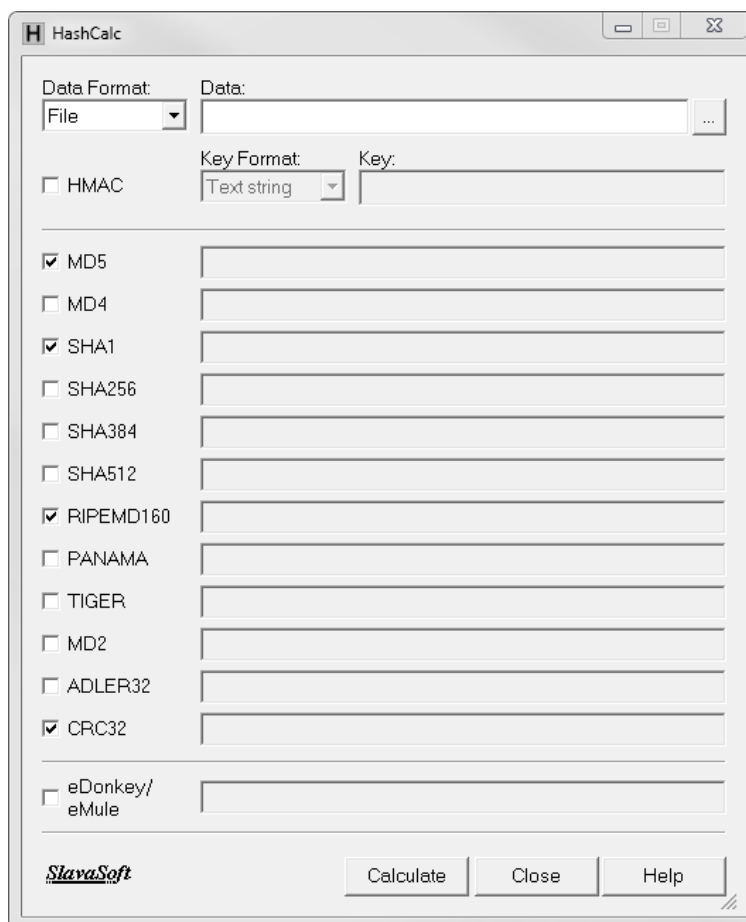
Product Name and Version	Operating System	Size	Download
HashCalc 2.02	Windows 95/98/Me/NT/2000/XP	468KB	Download
FSUM 2.52	Windows 95/98/Me/NT/2000/XP	92KB	Download

Copyright © 2016 SlavaSoft Inc. All rights reserved.

- б. Щелкните **Download (Загрузить)** в строке **HashCalc 2.02**.
- с. Откройте архив **hashcalc.zip** и запустите находящийся в нем файл **setup.exe**.



- d. Следуйте инструкциям мастера установки, чтобы установить HashCalc. Если в процессе установки возникнут вопросы, обратитесь за помощью к инструктору.
- e. Нажмите **Finish (Завершить)** на последнем экране и закройте файл **README**, если он открыт. При желании можно прочитать этот файл.
- f. Теперь программа HashCalc установлена и запущена.



Шаг 3: Вычислите хэш файла Hash.txt

- a. Задайте следующие параметры в HashCalc.
 - 1) Формат данных: **File**.
 - 2) Данные: щелкните кнопку ... рядом с полем Data (Данные), перейдите на **Desktop** и выберите файл **Hash.txt**.
 - 3) Снимите флажок **HMAC**.
 - 4) Снимите флажки со всех типов хэшей, кроме **MD5**.
- b. Нажмите кнопку **Calculate (Рассчитать)**.

Какое значение указано рядом с **MD5**?



Шаг 4: Внесите изменения в файл Hash.txt

- a. Перейдите на **Desktop** и откройте файл **Hash.txt**.
- b. Внесите любое небольшое изменение в текст, например удалите букву или добавьте пробел или точку.
- c. Щелкните **File > Save (Файл > Сохранить)** и закройте **Notepad**.

Шаг 5: Вычислите новый хэш файла Hash.txt

- a. Снова щелкните кнопку **Calculate (Рассчитать)** в программе HashCalc.

Какое значение указано рядом с **MD5**?



Отличается ли это значение от значения, записанного в шаге 3?



- b. Поставьте флажки рядом со всеми остальными типами хэша.
- c. Щелкните **Calculate (Рассчитать)**.
- d. Обратите внимание, что для многих хэш-функций созданы хэши разной длины. Почему?

