

Лабораторна робота. Порівняння даних за допомогою хешу

Цілі та задачі

Використати програму хешування для перевірки цілісності даних.

Довідкова інформація/Сценарій

Важливо виявляти, пошкодження або підмінену дані. Програма хешування може бути використана для перевірки, чи змінилися дані, чи вони залишилися незмінними. Програма хешування виконує хеш-функцію на даних або файлі, та повертає значення (як правило, набагато коротше) . Є багато різних хеш-функцій, деякі дуже прості, а деякі дуже складні. Коли однакова хеш-функція виконується з однаковими даними, то значення, що повертається, завжди однакове. Якщо з даними відбуваються будь-які зміни, то повернене значення хешу буде іншим.

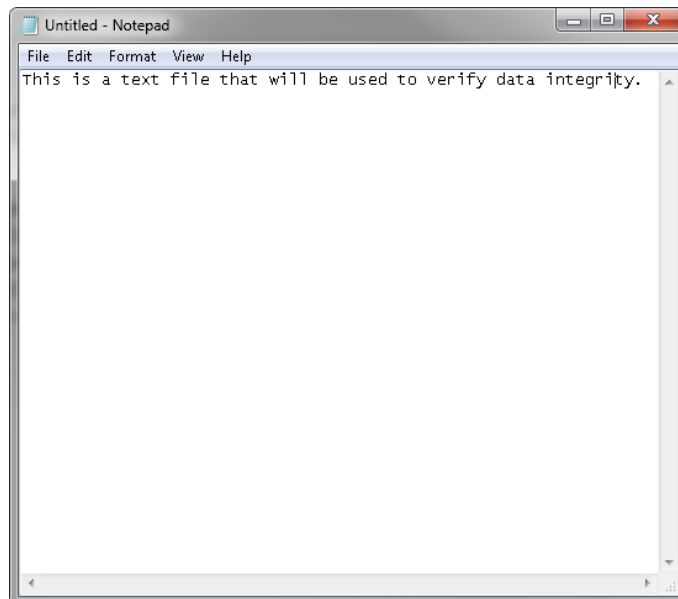
Примітка: Для встановлення Windows програм вам знадобляться відповідні привілеї та деякі знання.

Необхідні ресурси

- ПК з доступом до Інтернету

Крок 1: Створіть текстовий файл

- Знайдіть на своєму комп'ютері програму Блокнот (Notepad) і відкрийте її.
- Введіть текст у програмі.



- Виберіть **Файл > Зберегти (File > Save)**.
- Перейдіть до **Робочого столу**
- Введіть **Hash** у поле **Ім'я файлу: (File name:)** і натисніть **Зберегти (Save)**.

Крок 2: Встановіть HashCalc

а Відкрийте веб-браузер і перейдіть за посиланням <http://www.slavaSoft.com/download.htm>.

SlavaSoft *Where quality software is just a click away.*

Home | Products | **Downloads** | Purchase | Support February 19, 2016

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

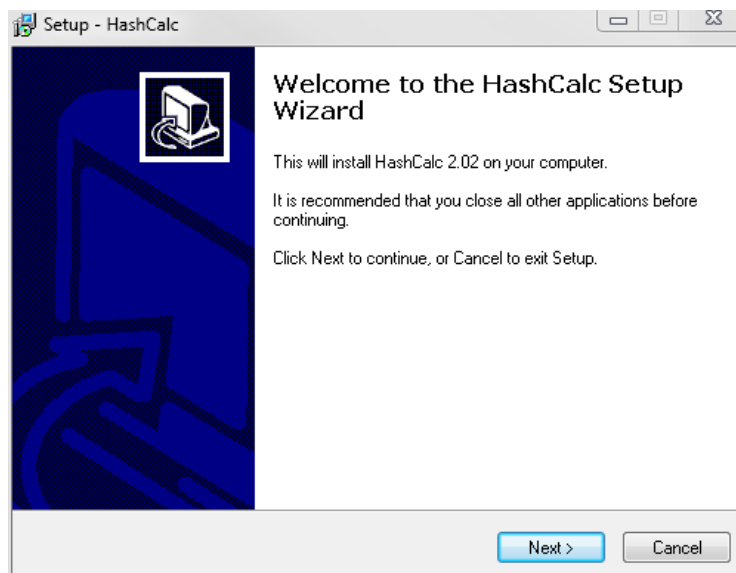
You can download the following products and **use them for free**.

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 Натисніть **Завантажити (Download)** у рядку **HashCalc**.

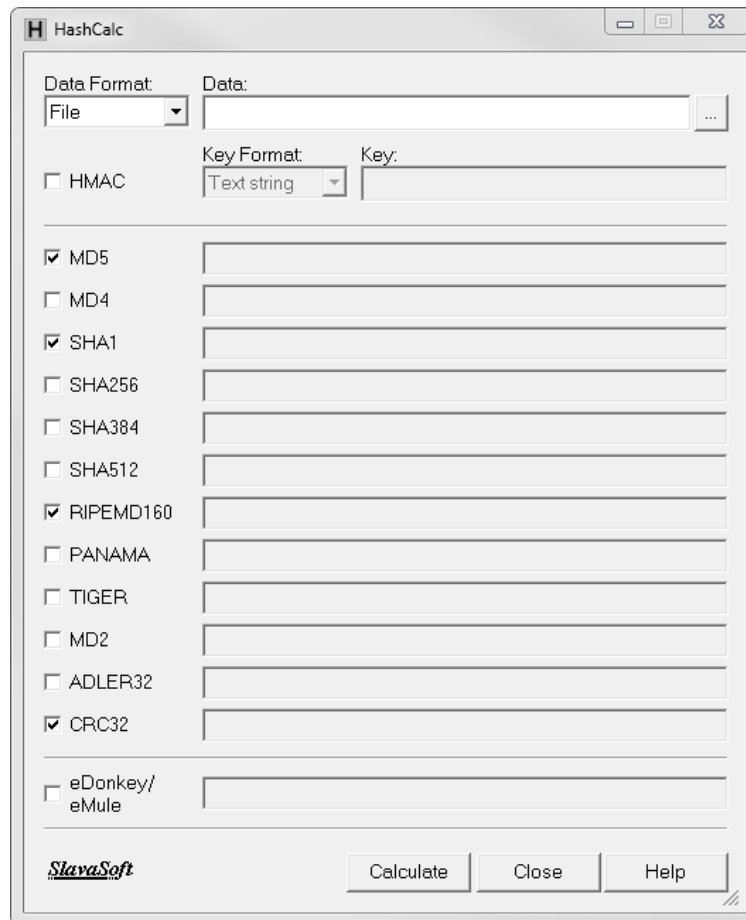
с Відкрийте **hashcalc.zip** файл та запустіть файл **setup.exe** всередині.



д Дотримуйтесь вказівок Майстра установки (Installation wizard), щоб встановити HashCalc.

е Натисніть кнопку **Готово (Finish)** на останньому екрані та закрийте файл **README**, якщо він відкритий. Ви можете прочитати файл, якщо захочете.

г HashCalc тепер встановлено та запущено.



Крок 3: Обчисліть хеш файлу Hash.txt

- a. Вкажіть наступні елементи у HashCalc:
 - 1) Формат даних (Data Format): **Файл (File)**.
 - 2) Дані: натисніть ...Поруч із полем Дані (Data), перейдіть на **Робочий стіл (Desktop)** і виберіть файл **Hash.txt**.
 - 3) Зніміть прапорець **HMAC**
 - 4) Зніміть усі типи хешів, крім **MD5**
- b. Натисніть кнопку **Обчислити (Calculate)**.
Яке значення поряд із **MD5**?

Крок 4: Внесіть зміни у файлі Hash.txt

- a. Перейдіть на **Робочий стіл** і відкрийте файл **Hash.txt**.

- b. Зробіть невелику зміну тексту, наприклад, видалення літери або додавання пробілу.
- c. Натисніть **Файл > Зберегти (File > Save)** та закрийте **Блокнот**.

Крок 5: Обчисліть новий хеш файлу Hash.txt

- a. Знову натисніть кнопку **Обчислити (Calculate)** в HashCalc.
Яке значення поряд із **MD5**?

Чи значення відрізняється від значення, що одержано на кроці 3?

- b. Поставте прапорець біля усіх типів хеш-функцій.
 - c. Натисніть **Обчислити (Calculate)**
 - d. Зверніть увагу, що багато типів хеш-функцій створюють хеш різної довжини. Чому?
-