Ćwiczenie – Porównaj dane z wynikiem funkcji haszującej (Wersja dla nauczyciela)

**Informacja dla nauczyciela**: Tekst oznaczony kolorem czerwonym lub wyróżniony kolorem szarym jest dostępny wyłącznie w wersji dla nauczyciela.

1. Zadania

Użyj narzędzia haszującego do sprawdzenia integralności danych.

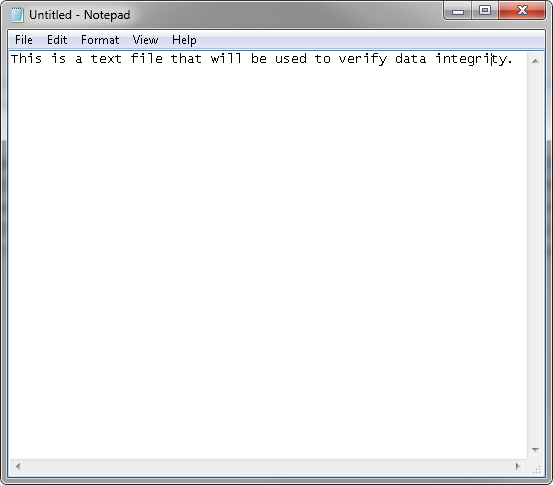
1. Wprowadzenie

Ważne jest, aby dostrzec uszkodzenie lub modyfikację danych. Program haszujący może być użyty do sprawdzenia, czy dane zostały zmodyfikowane, czy też pozostały niezmienione. Program haszujący oblicza funkcję skrótu dla pliku, która zwraca (zazwyczaj znacznie krótszą) wartość. Istnieje wiele różnych funkcji skrótu, niektóre są bardzo proste, inne – bardzo złożone. Gdy funkcja haszująca jest stosowana do tych samych danych, zwracana wartość jest zawsze taka sama. Jeśli zostanie wykonana jakakolwiek zmiana danych, zwrócona wartość będzie inna.

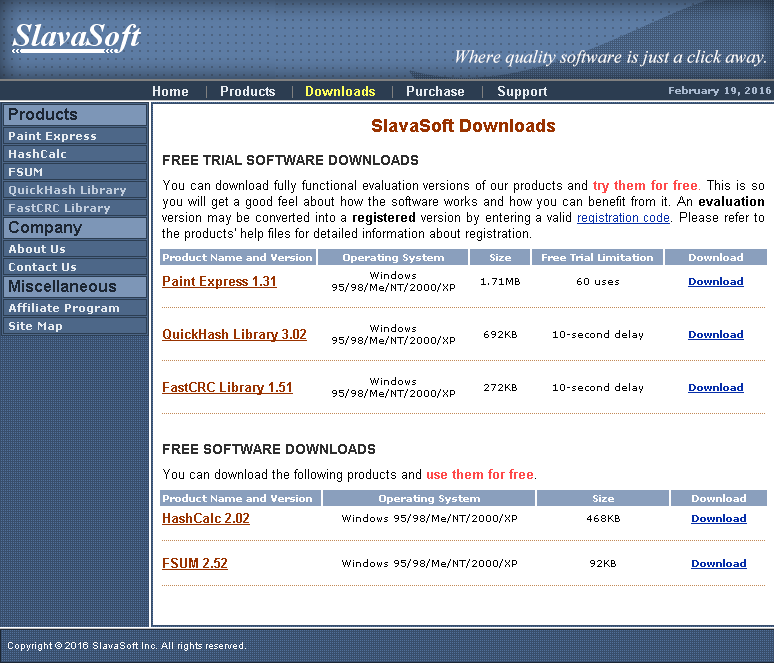
**Uwaga**: Będą potrzebne uprawnienia do instalacji oraz trochę wiedzy na temat procesu instalacji programów w systemie Windows.

1. Wymagane zasoby

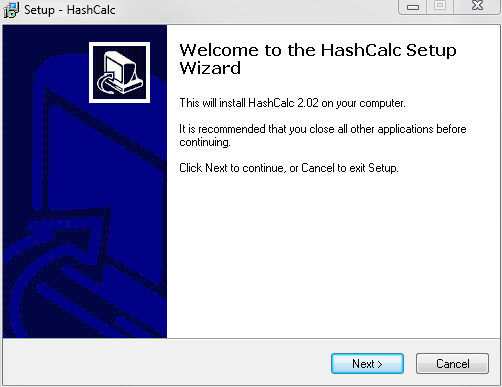
* Komputer z dostępem do Internetu
  1. Utwórz plik tekstowy
     1. Wyszukaj w komputerze program Notatnik i otwórz go.
     2. Wpisz dowolny tekst w programie.



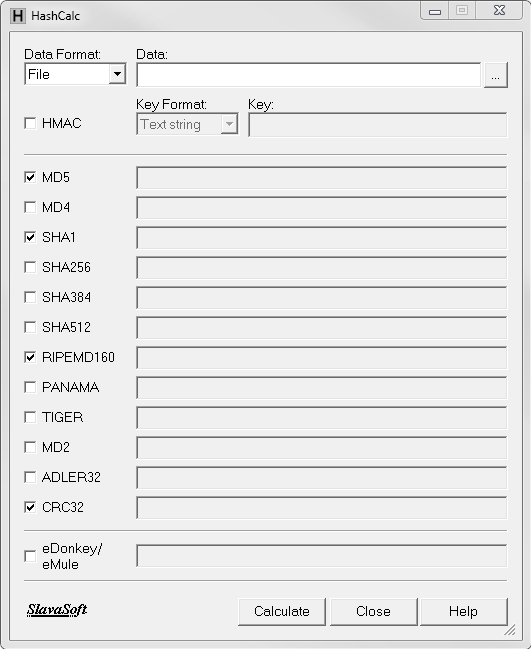
* + 1. Wybierz **Plik > Zapisz**.
    2. Przejdź do **Pulpitu**.
    3. Wpisz **Hash** w **polu Nazwa pliku:** i kliknij **Zapisz**.
  1. Zainstaluj narzędzie HashCalc
     1. Otwórz przeglądarkę internetową i przejdź do <http://www.slavasoft.com/download.htm>.



* + 1. Kliknij **Download** w wierszu **HashCalc 2.02**.
    2. Otwórz archiwum **hashcalc.zip** i uruchom plik **setup.exe** znajdujący się w środku.



* + 1. Postępuj zgodnie z instrukcjami kreatora instalacji, aby zainstalować HashCalc.
    2. Naciśnij przycisk **Finish** na ostatnim ekranie i zamknij plik **README**, jeżeli został otworzony. Możesz zapoznać się z zawartością pliku.
    3. HashCalc został zainstalowany i uruchomiony.



* 1. Oblicz wartość funkcji haszującej dla pliku Hash.txt.
     1. Ustaw następujące opcje w programie HashCalc:
        1. Data Format: **File**.
        2. Data: naciśnij przycisk **…** znajdujący się obok pola „Data", a następnie przejdź do **pulpitu** i wybierz plik **Hash.txt**.
        3. Odznacz **HMAC**.
        4. Odznacz wszystkie funkcje haszujące oprócz **MD5**.
     2. Naciśnij przycisk **Calculate**.

Jaka jest wartość, która wyświetla się obok **MD5**?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Odpowiedzi mogą się różnić. Przykład: 82e8ac8d4ae929c79e1ce4cf1f0691f4

* 1. Edytuj plik Hash.txt i dokonaj w nim dowolnej zmiany.
     1. Przejdź do **pulpitu** i otwórz plik **Hash.txt**.
     2. Dokonaj drobnej zmiany w tekście, na przykład usuń literę, dodaj spację lub kropkę.
     3. Naciśnij **Plik > Zapisz**, a następnie zamknij **Notatnik**.
  2. Oblicz nową wartość funkcji haszującej dla pliku Hash.txt.
     1. Ponownie kliknij przycisk **Calculate** w programie HashCalc.

Jaka jest wartość, która wyświetla się obok **MD5**?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Wartości funkcji haszującej mogą się zmieniać, ale będą inne niż w kroku 3. Przykład: fb53ad826cefac1dbee8f583a66b7bf4

Czy wartość jest inna niż wartość zarejestrowana w kroku 3?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tak.

* + 1. Zaznacz wszystkie funkcje haszujące.
    2. Kliknij **Calculate**.
    3. Zauważ, że funkcje haszujące tworzą hasze o różnych długościach. Dlaczego tak jest?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Funkcje haszujące używają różnych liczb bitów do wygenerowania wartości hasza.