Atelier – Comparer les données hachées (Version du formateur)

**Remarque à l’intention du formateur :** le texte en rouge ou surligné en gris apparaît uniquement dans la version du formateur.

1. Objectifs

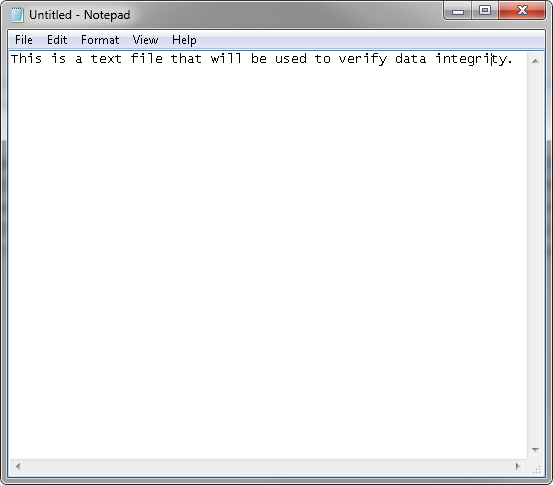
Utilisez un programme de condensation pour vérifier l’intégrité des données.

1. Contexte/scénario

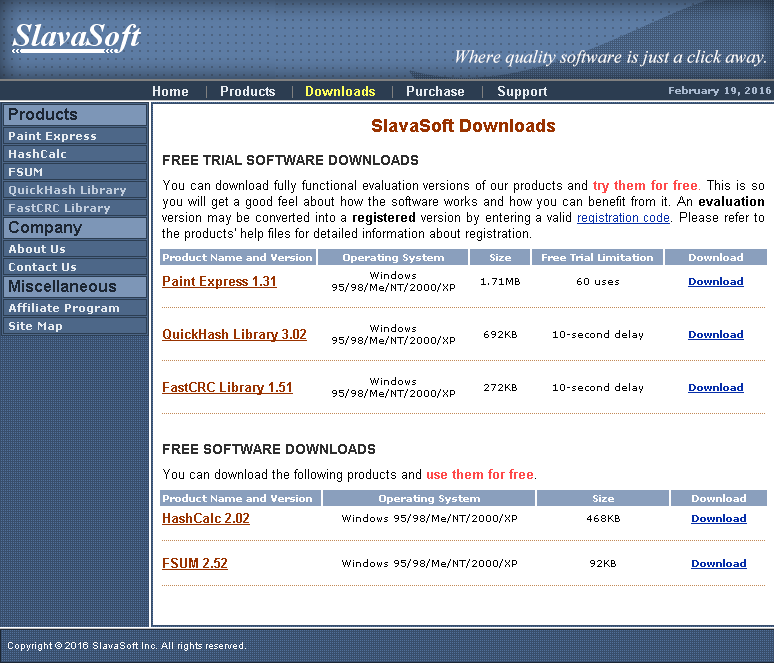
Il est important de comprendre si les données ont été corrompues ou si ces dernières ont été modifiées. Un programme de condensation peut être utilisé pour vérifier si les données ont été falsifiées ou non. Un programme de condensation exécute une fonction de hachage sur les données ou sur un fichier, qui génère une valeur (souvent très réduite). Il existe de nombreux types de fonctions de hachage, certaines très simples et d’autres très complexes. Si le même algorithme est exécuté sur le même lot de données, la valeur générée reste la même. Si les données ont été modifiées, la valeur hachée générée sera différente.

1. Ressources requises

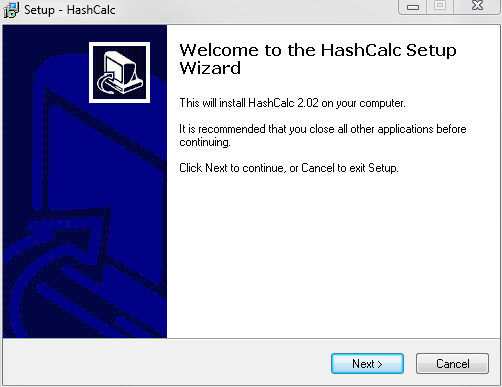
* Un PC avec un accès Internet
  1. Créer un fichier texte
     1. Recherchez le programme Bloc-notes sur votre ordinateur et ouvrez-le.
     2. Tapez un texte dans le programme.



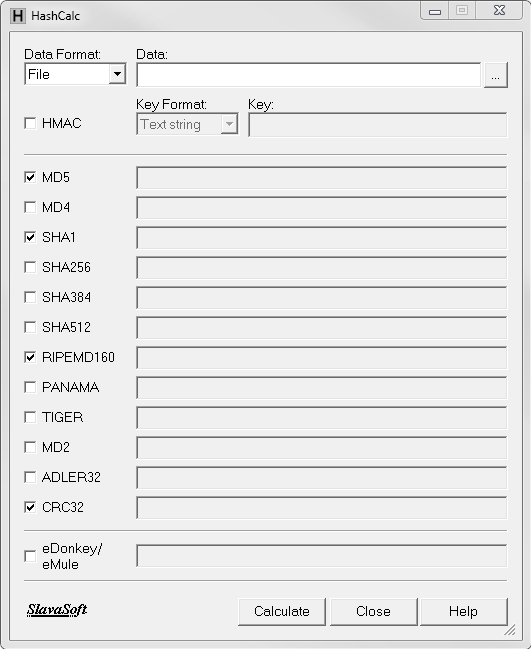
* + 1. Sélectionnez **Fichier > Enregistrer**.
    2. Accédez au **Bureau**.
    3. Tapez **Hash** dans le champ **Nom de fichier :** et cliquez sur **Enregistrer**.
  1. Installer HashCalc
     1. Ouvrez un navigateur Web et accédez à l’adresse <http://www.slavasoft.com/download.htm>.



* + 1. Cliquez sur **Download** (Télécharger) dans la ligne **HashCalc 2.02**.
    2. Ouvrez le fichier **hashcalc.zip** et exécutez le fichier d’installation **setup.exe** intégré.



* + 1. Suivez les instructions de l’assistant d’installation de HashCalc. Demandez l’aide de votre instructeur pour toute question concernant l’installation.
    2. Cliquez sur **Finish** (Terminer) dans la dernière fenêtre contextuelle et fermez le fichier **README** (Lisez-moi) qui s’affiche. Vous pouvez lire le fichier si vous le souhaitez.
    3. HashCalc est désormais installé et opérationnel.



* 1. Calculer un algorithme pour le fichier Hash.txt
     1. Configurez les éléments suivants dans HashCalc :
        1. Format de données : **File** (Fichier).
        2. Données : cliquez sur le bouton **…** à côté du champ Data (Données), accédez au **Bureau** et sélectionnez le fichier **Hash.txt**.
        3. Décochez **HMAC**.
        4. Décochez tous les types d’algorithme, sauf **MD5**.
     2. Cliquez sur le bouton **Calculate** (Calculer).

Quelle est la valeur à côté de **MD5** ?

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

Les réponses peuvent varier. Exemple : 82e8ac8d4ae929c79e1ce4cf1f0691f4

* 1. Modifier le fichier Hash.txt
     1. Accédez au **Bureau** et ouvrez le fichier **Hash.txt**.
     2. Modifiez un peu le texte, comme supprimer une lettre ou ajouter un espace ou un point.
     3. Cliquez sur **Fichier > Enregistrer**, et fermer le **Bloc-notes**.
  2. Calculer un nouvel algorithme pour le fichier Hash.txt
     1. Cliquez de nouveau sur le bouton **Calculate** (Calculer) dans HashCalc.

Quelle est la valeur à côté de **MD5** ?

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

Les réponses peuvent varier, mais elles seront différentes de l’étape 3. Exemple : fb53ad826cefac1dbee8f583a66b7bf4

La valeur est-elle différente de celle enregistrée à l’étape 3 ?

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

Oui.

* + 1. Cochez tous les types d’algorithme.
    2. Cliquez sur **Calculer**.
    3. Remarquez que certains types d’algorithme créent un algorithme de différente longueur. Pourquoi ?

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

De nombreux hachages sont produits en utilisant un nombre de bits différent.