**Aubrée Romain** **Sotoca**
**09/10/2025**

**Groupe 1**

# Bloc 3 TP-5

# Partie 1 :

## 1. Création du fichier Hash.txt

Création d’un fichier Hash.txt avec du contenue à l'intérieur.


Fichier Edition Format Affichage Aide
Test Hash Cours 08/10

## 2. Installation d’un logiciel de calcul de hachage

Installation du logiciel HashCalc, un programme qui calcule le hachage.

Le hachage transforme un fichier ou un texte en une suite de caractères unique appelée empreinte.

Cette empreinte permet de vérifier si le fichier a changé ou pas.

# 3. Calcul du *hash*

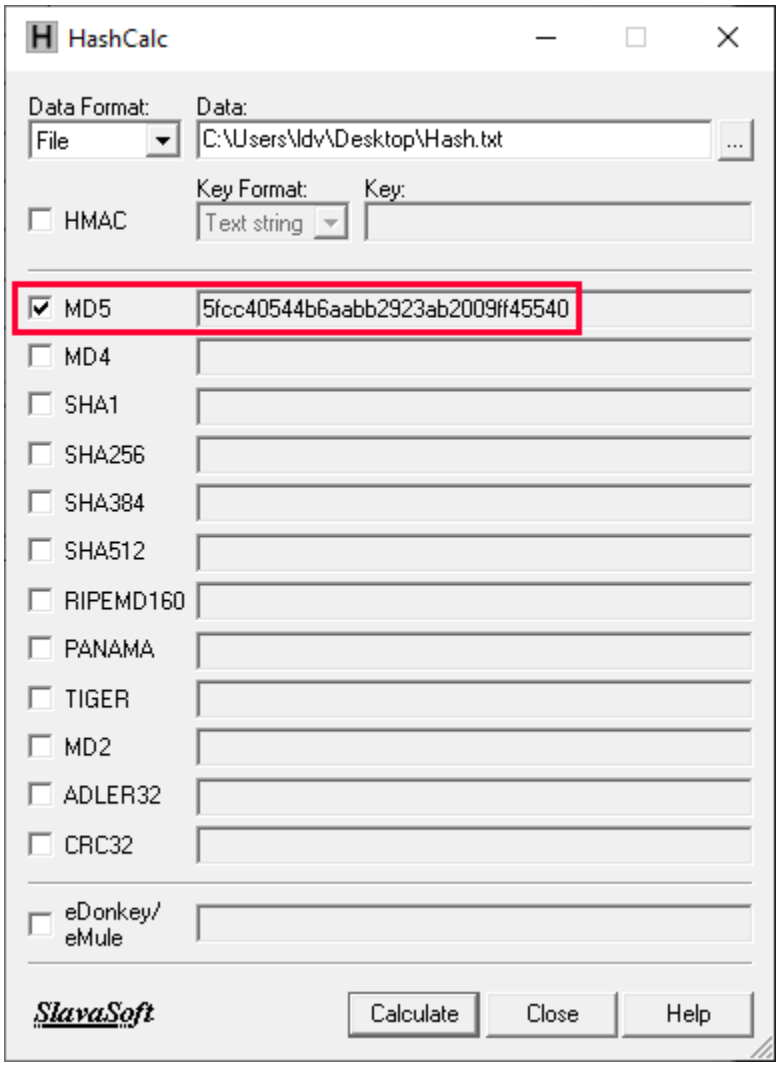
-Sélection “***File***”

-Sélection du Hash.txt pour “***Data***”

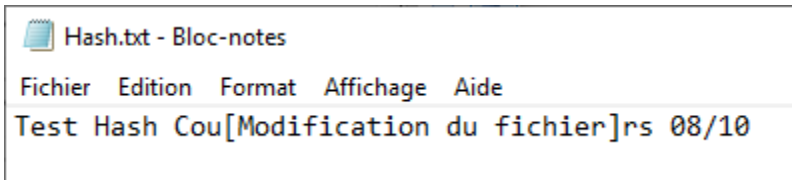
-Décochage de **HMAC**

-Décochage de tout sauf **MD5**

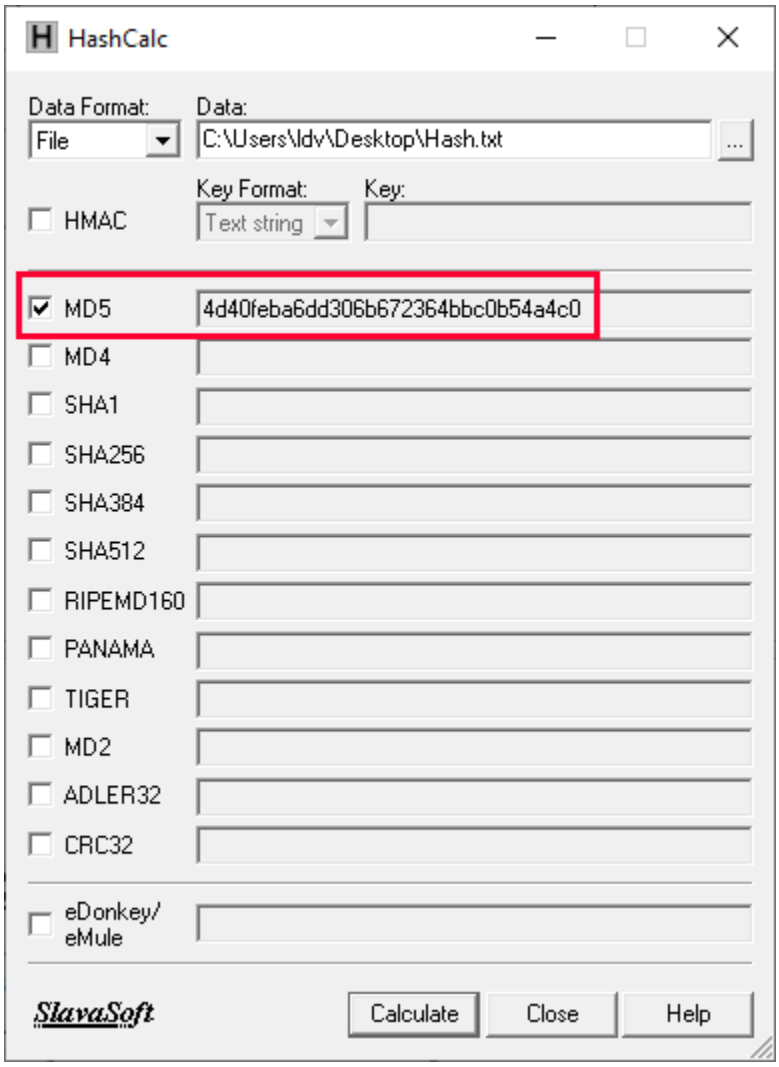
Voici la valeur obtenu pour **MD5**:



# 4. Modification du fichier Hash.txt et nouveau calcul



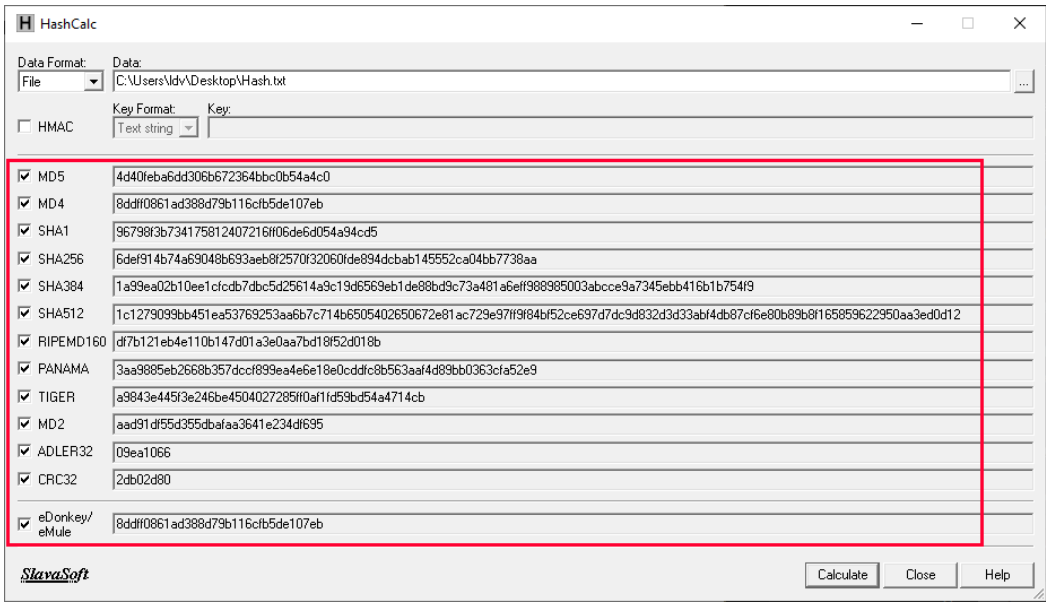

Nouveau résultat de **MD5** après la modification:




La valeur est différente de celle enregistrée à l'étape 3 parce que le contenu du fichier a été modifié. Même un petit changement dans le texte change complètement l'empreinte **MD5**.

# 5. Résultats avec tous les types d'algorithme

Voici les résultat avec tout les type d'algorithme:




Les algorithmes de hachage donnent des résultats (ou empreintes) de tailles différentes parce qu'ils sont faits de manières différentes. Chaque algorithme (comme MD5, SHA-1, SHA-256…) a sa propre méthode de calcul, et donc il crée un code plus ou moins long.

-**MD5** fait un code court (32 caractères)

-**SHA-1** un peu plus long (40 caractères)

-**SHA-256** encore plus long (64 caractères)

-**SHA-512** très long (128 caractères)

Plus le code est long, plus il est difficile à casser ou à pirater.

# Partie 2 :

## 6. Liste d’entreprises victimes d'une faille

| Date de l’incident | Entreprise touché | Nombre de victimes Données volées | Méthodes utilisées Mesure(s) de protection prise(s) | Source de référence |
|---|---|---|---|---|
| 2017 | Equifax | ~147 millions (États-Unis). Noms, dates de naissance, numéros de sécurité sociale, adresses, numéros de permis | Exploitation d’une vulnérabilité non corrigée (Apache Struts) sur un serveur public. Correctifs, audits de sécurité, offre de surveillance de crédit aux victimes, amendes et accords légaux | Communiqués officiels + grandes agences de presse (2017–2019) |
| 2013–2014 (annoncé 2016) | Yahoo | Jusqu’à ~3 milliards de comptes (différents incidents). Adresses e-mail, mots de passe chiffrés/clair selon cas, questions/réponses de sécurité. | Compromission des bases utilisateurs via accès non autorisé aux systèmes internes. Réinitialisation des mots de passe, amélioration des contrôles d’accès, | Rapports officiels et enquêtes médiatiques (2016–2017) |

| | | | | |
|---|---|---|---|---|
| | | | enquêtes forensiques | |
| 2018 (annoncé 2018–2019) | Marriott / Starwood | ~500 millions de clients. Noms, adresses, numéros de passeport, e-mails, détails de réservations | Maintien d'accès non détecté à une base cryptée depuis plusieurs années (compromission prolongée). Notifications clients, renforcement des accès, collaboration avec autorités, offres de surveillance | Communiqués Marriott + médias (2018–2019) |
| 2019 (annoncé juillet 2019) | Capital One | ~100 millions (États-Unis) + 6 millions (Canada) Noms, adresses, numéros de téléphone, numéros de sécurité sociale partiels, informations de crédit | Exploitation d'une mauvaise configuration cloud / accès par un attaquant qui a récupéré des données via des instances AWS. Correction de la configuration, coopération policière, notification des clients, renforcement IAM et revue cloud | Communiqués Capital One + enquêtes journaux (2019) |

| | | | | |
|---|---|---|---|---|
| 2020 (découverte fin 2020) | SolarWinds (attaque supply-chain) | Centaines d'organisations (dont agences gouvernementales et entreprises). Accès réseau, données sensibles selon la cible (varie) | Compromission de la chaîne d'approvisionnement : mise à jour logicielle légitime contenant un backdoor (insertion malveillante dans une mise à jour). Retrait des mises à jour compromises, audits massifs, renforcement de la sécurité des chaînes d'approvisionnement logicielles | Rapports gouvernementaux + médias tech (2020–2021) |

# 7. Conclusion

On a vu que même un petit changement dans un fichier change complètement son empreinte, car l'algorithme regarde tout le fichier. Chaque algorithme fait une empreinte de taille différente selon sa méthode. Ces empreintes aident à vérifier si un fichier a été modifié.