Aouinine Abdelhak
BTS SIO 1
Groupe SISR

Les empreintes cryptographiques MD5/SHA1

Empreinte MD5

D’abord on se met en mode super admin avec la commande « su » et le mot de passe .
On tape la commande « echo bonjour > fichier1 » dans le terminale . Après pour calculé le résumé MD5 de fichier 1, on met la commande md5sum donc on vas écrire md5sum fichier1 « md5sum fichier1 ». On fait la même chose pour le fichier 2 et 3 .

fichier1 :

```
root@debian:/home/administrateur# echo bonjour > fichier1
root@debian:/home/administrateur# md5sum fichier1
94baaad4d1347ec6e15ae35c88ee8bc8  fichier1
```

fichier2 :

```
root@debian:/home/administrateur# echo bonjour > fichier2
root@debian:/home/administrateur# md5sum fichier2
94baaad4d1347ec6e15ae35c88ee8bc8  fichier2
```

fichier3 :

```
root@debian:/home/administrateur# echo bonjour > fichier3
root@debian:/home/administrateur# md5sum fichier3
94baaad4d1347ec6e15ae35c88ee8bc8  fichier3
```

- On remarque que les trois fichiers ont la même résumé .

Quelques subtilités...

On tape ma commande « echo bonjour | md5sum » sur le site de calculateur MD5 « http://www.md5.cz/ » , et on trouve un résumé différent par rapport aux fichiers d'avants .

On a taper la commande sur le terminale :

```
root@debian:/home/administrateur# echo bonjour | md5sum
94baaad4d1347ec6e15ae35c88ee8bc8  -
```

- On a des résumés différents pourtant on a taper la même commande .

On tape aussi la commande « echo -n bonjour | md5sum » sur le calculateur MD5 et le terminale .


```
root@debian:/home/administrateur# echo -n bonjour | md5sum
f02368945726d5fc2a14eb576f7276c0  -
```

- Le paramètre « -n » sert à supprimé le retour à la ligne .

Empreinte SHA1

On tape la commande « echo bonjour > fichier4 » dans le terminale, après on calcule le résumé SHA1 du fichier4 avec la commande «sha1sum fichir4 ». On fait la même chose pour le fichier 5 .

fichier 4 :

```
root@debian:/home/administrateur# echo bonjour > fichier4
root@debian:/home/administrateur# sha1sum fichier4
e7bc546316d2d0ec13a2d3117b13468f5e939f95  fichier4
```

fichier 5 :

```
root@debian:/home/administrateur# echo bonjour > fichier5
root@debian:/home/administrateur# sha1sum fichier5
e7bc546316d2d0ec13a2d3117b13468f5e939f95  fichier5
```

- On remarque que le fichier 4 et le fichier 5 ont le même résumé .

On fait la même chose pour le fichier 6 et on voit qu’on a le même résumé par rapport au fichier4 et fichier 5 quand on utilise la commande sha1sum .

```
root@debian:/home/administrateur# echo bonjour > fichier6
root@debian:/home/administrateur# sha1sum fichier6
e7bc546316d2d0ec13a2d3117b13468f5e939f95  fichier6
```

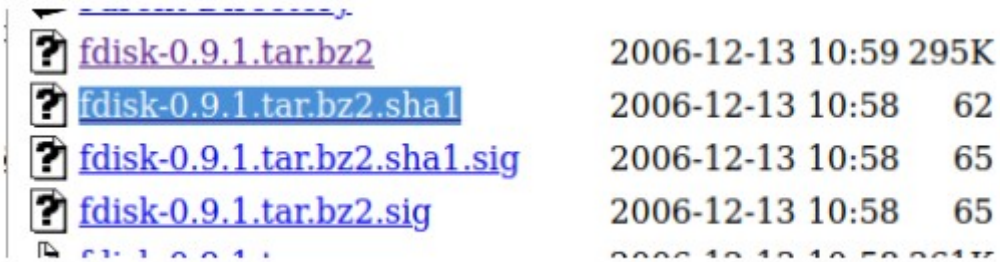
Comparez les résumés de "sum", "md5sum", "sha1" et "sh512sum"

```
root@debian:/home/administrateur# sum fichier3
45178    1
root@debian:/home/administrateur# md5sum fichier3
94baaad4d1347ec6e15ae35c88ee8bc8  fichier3
root@debian:/home/administrateur# sha1sum fichier3
e7bc546316d2d0ec13a2d3117b13468f5e939f95  fichier3
root@debian:/home/administrateur# sha512sum fichier3
a514669228bdc39ecf8a9a6c9157964ff32b53365601a59b6c40d151303988ea18b338c684d40fcdbef9b2eeaa388bc2332e3a2585b06bb349178c71050008e7  fichier3
root@debian:/home/administrateur#
```

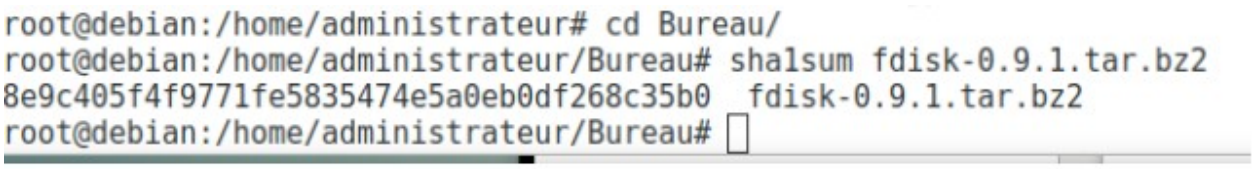
- On remarque que malgré qu’on a le meme fichier, mais on change les commande. Le résumé est différent .

Vérifier l'intégrité d'un logiciel téléchargé

On vas sur le liens « ftp://ftp.gnu.org/gnu/fdisk/ » et on télécharge un l'utilitaire Linux .



Après on vas sur la terminale et on tape des commandes pour avoir un résumé .



<u>Petit exercice sympa !</u>

Le mot qui correspond avec ce résumé «effd456daab1ca177fdc0580a63eb4108cdf9335cfe70ddd2e73d399b46a70d3 » est : sandydeluz
- J’ai utiliser le logiciel SHA256online .