

## Partie A :

```
[analyst@secOps ~]$ cd /home/analyst/lab.support.files/
[analyst@secOps lab.support.files]$ cat letter_to_grandma.txt
Hi Grandma,
I am writing this letter to thank you for the chocolate chip cookies you sent me. I got them this morning and I have already eaten half of the box! They are absolutely delicious!

I wish you all the best. Love,
Your cookie-eater grandchild.

[analyst@secOps lab.support.files]$ openssl sha256 letter_to_grandma.txt
SHA256(letter_to_grandma.txt)= deff9c9bbece44866796ff6cf21f2612fbb77aa1b2515a900bafb29be118080b
[analyst@secOps lab.support.files]$
```

```
Hi Grandpa,
I am writing this letter to thank you for the chocolate chip cookies you sent me. I got them this morning and I have already eaten half of the box! They are absolutely delicious

I wish you all the best. Love,
Your cookie-eater grandchild.
```

```
SHA256(letter_to_grandma.txt)= deff9c9bbece44866796ff6cf21f2612fbb77aa1b2515a900bafb29be118080b
[analyst@secOps lab.support.files]$ nano letter_to_grandma.txt
[analyst@secOps lab.support.files]$ openssl sha256 letter_to_grandma.txt
SHA256(letter_to_grandma.txt)= 43302c4500b7c4b8e574ba27a59d83267812493c029fd054c9242f3ac73100bc
[analyst@secOps lab.support.files]$
```

Le hash est totalement différent du précédent hash puisque son contenu a été modifié.

```
SHA256(letter_to_grandma.txt)= 43302c4500b7c4b8e574ba27a59d83267812493c029fd054c9242f3ac73100bc
[analyst@sec0ps lab.support.files]$ sha512 letter_to_grandma.txt
bash: sha512: command not found
[analyst@sec0ps lab.support.files]$ openssl sha512 letter_to_grandma.txt
SHA512(letter_to_grandma.txt)= 7c35db79a06aa30ae0f6de33f2322fd419560ee9af9cedeb6e251f2f1c4e99e0bbe5d2fc32ce501468891150e3be7e288e3e568450812980c9f8288e3103a1d3
[analyst@sec0ps lab.support.files]$ openssl sha256sum letter_to_grandma.txt
Invalid command 'sha256sum'; type "help" for a list.
[analyst@sec0ps lab.support.files]$ sha256sum letter_to_grandma.txt
43302c4500b7c4b8e574ba27a59d83267812493c029fd054c9242f3ac73100bc  letter_to_grandma.txt
[analyst@sec0ps lab.support.files]$ sha512sum letter_to_grandma.txt
7c35db79a06aa30ae0f6de33f2322fd419560ee9af9cedeb6e251f2f1c4e99e0bbe5d2fc32ce501468891150e3be7e288e3e568450812980c9f8288e3103a1d3  letter_to_grandma.txt
[analyst@sec0ps lab.support.files]$
```

On remarque que sha256 correspond à sha256sum et idem pour sha512 et sha512sum. Le sha modifie le hachage utilisé pour letter\_to\_grandma.txt ce qui explique la différence entre sha256 et sha512.

Cependant, sha256sum nous permet simplement d'ouvrir sha256 sans passer par « openssl » ce qui ne modifie rien entre sha256 et sha256sum.

## Partie 2 :

```
7c35db79a06aa308e0f6de33f2322fd419560ee9af9cedeb6e251f2f1c4e99e0bbe5d2fc32ce501468891150e3be7e288e3e568450812980c9f8288e3103a1d3 letter_to_grandma.txt
[analyst@sec0ps lab.support.files]$ cat sample.img_SHA256.sig
c56c4724c26eb0157963c0d62b76422116be31804a39c82fd44ddf0ca5013e6a
[analyst@sec0ps lab.support.files]$ sha256sum sample.img
c56c4724c26eb0157963c0d62b76422116be31804a39c82fd44ddf0ca5013e6a sample.img
[analyst@sec0ps lab.support.files]$
```

On remarque que la liste « c56c[...]13e6a » reste identique entre les deux commandes utilisées dans cette partie.

La seule exception étant dans la deuxième commande où « sample.img » s'affiche. On peut donc en déduire que la deuxième commande ne permet pas de télécharger une image.