

# INTEGRITY OF THE DATA



**How can we validate the integrity of the data?**

**How to verify if the data that was sent is equal to the data that was received?**

**How can i check if data has been altered?**

Those are the most frequent questions when we want to know if a file is legitimate, especially when it comes from websites. Among the methods to verify the integrity of the data, we have the hash, hashing is the process of converting and input of any lenght into a fix sized string of text, through a mathematical function.



Let's take a look with an practical case. Let's say that I want to download Kali Linux for a future pentest practice.

**KALI**  
BY OFFENSIVE SECURITY

Blog Downloads Training Documentation Community About Us

## Kali Linux Downloads

### Download Kali Linux Images

We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to download Kali Linux in its latest official release. For a release history, check our Kali Linux Releases page. Please note: You can find unofficial, untested weekly releases at <http://cdimage.kali.org/kali-weekly/>. Downloads are **rate limited to 5 concurrent connections**.

Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux 64-Bit (Installer)	Torrent	2020.4	4.1G	50492d761e408c2b5e22c8f253dd6f75c27e4bc84e33c2eff272476a0988fb02

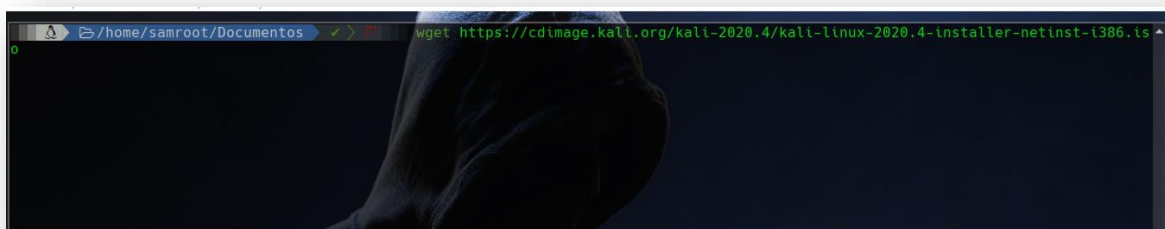
**NEW FOR 2020**

**OFFSEC**  
**NEW COURSE**

**OSEP**  
Evasion Techniques and Breaching Defenses

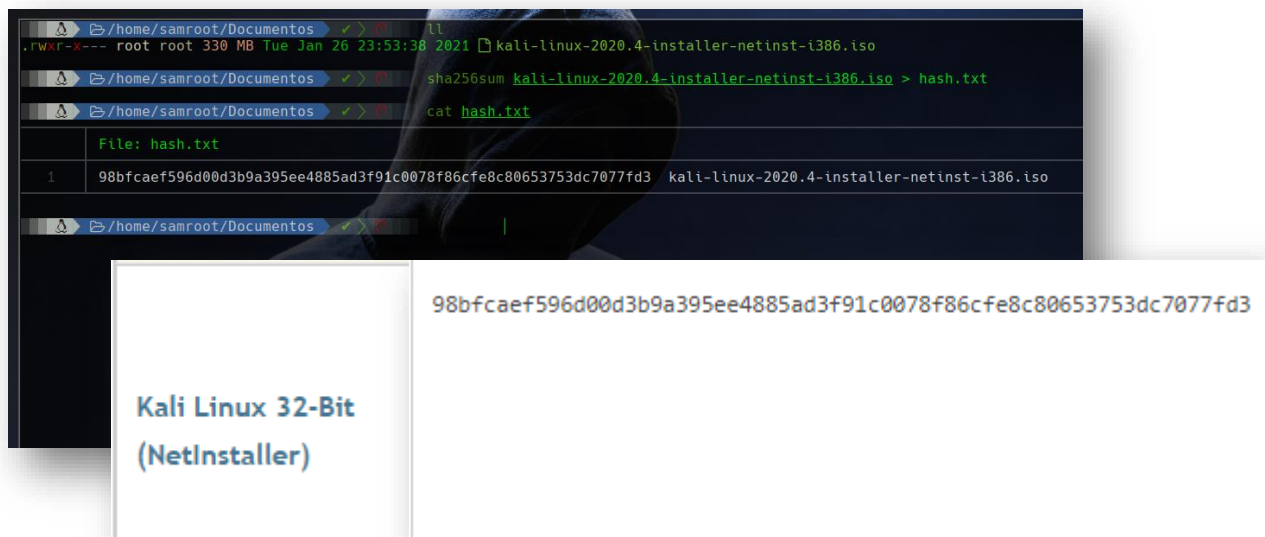
As we can see, we can find the name of the file and its hash value, in this case in sha256. So, we want to download the following image:

(Installer)				
Kali Linux 32-Bit (Live)	Torrent	2020.4	2.8G	10e81e2d1ed7bc100398871db45b628c11199a9901b1935bc56b5a8e9dc62667
Kali Linux 32-Bit (NetInstaller)	Torrent	2020.4	330M	98bfcaef596d00d3b9a395ee4885ad3f91c0078f86cfe8c80653753dc7077fd3
Kali Linux 64-bit VMware	Available on the Offensive Security VM Download Page			
Kali Linux 32-bit (PAE) VMware	Available on the Offensive Security VM Download Page			
Kali Linux 64-bit VirtualBox	Available on the Offensive Security VM Download Page			



```
wget https://cdimage.kali.org/kali-2020.4/kali-linux-2020.4-installer-netinst-i386.t
```

After downloading the file, we proceed to verify if the hash value is the same, and I can certify that the image has not been altered. we do this through the sha256sum command followed by the name of the file to which I am making the query. Let's take a look.



```
ll
-rwxr-x--- root root 330 MB Tue Jan 26 23:53:38 2021 kali-linux-2020.4-installer-netinst-i386.iso
sha256sum kali-linux-2020.4-installer-netinst-i386.iso > hash.txt
cat hash.txt
```

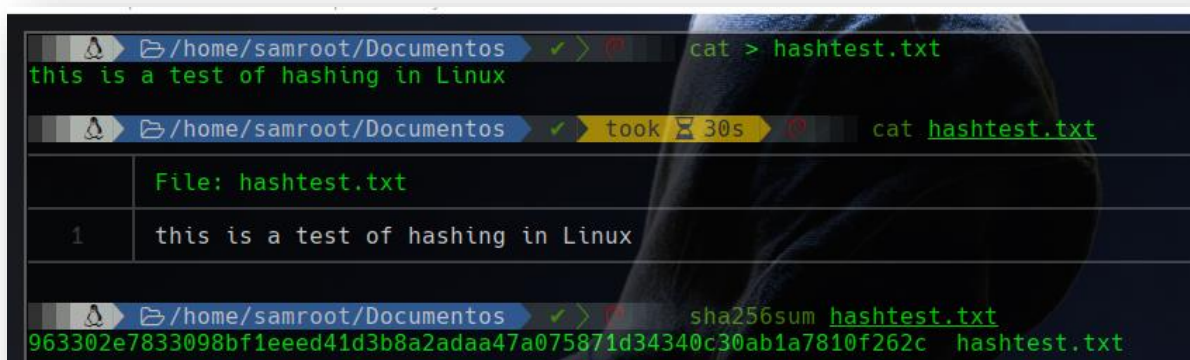
File: hash.txt	
1	98bfcaef596d00d3b9a395ee4885ad3f91c0078f86cfe8c80653753dc7077fd3 kali-linux-2020.4-installer-netinst-i386.iso

**Kali Linux 32-Bit  
(NetInstaller)**

98bfcaef596d00d3b9a395ee4885ad3f91c0078f86cfe8c80653753dc7077fd3

As we can see the hash is exactly the same, which means that the data has not been modified. But let's try some example to see the change of the value.

First let's create a txt file named hashtest.txt with the following content **"This is a test of hashing in Linux"** then we check the file with the command cat, to see its content without opening the file with any editor. Then we can calculate the hash with the command sha256sum and the output will be a string.

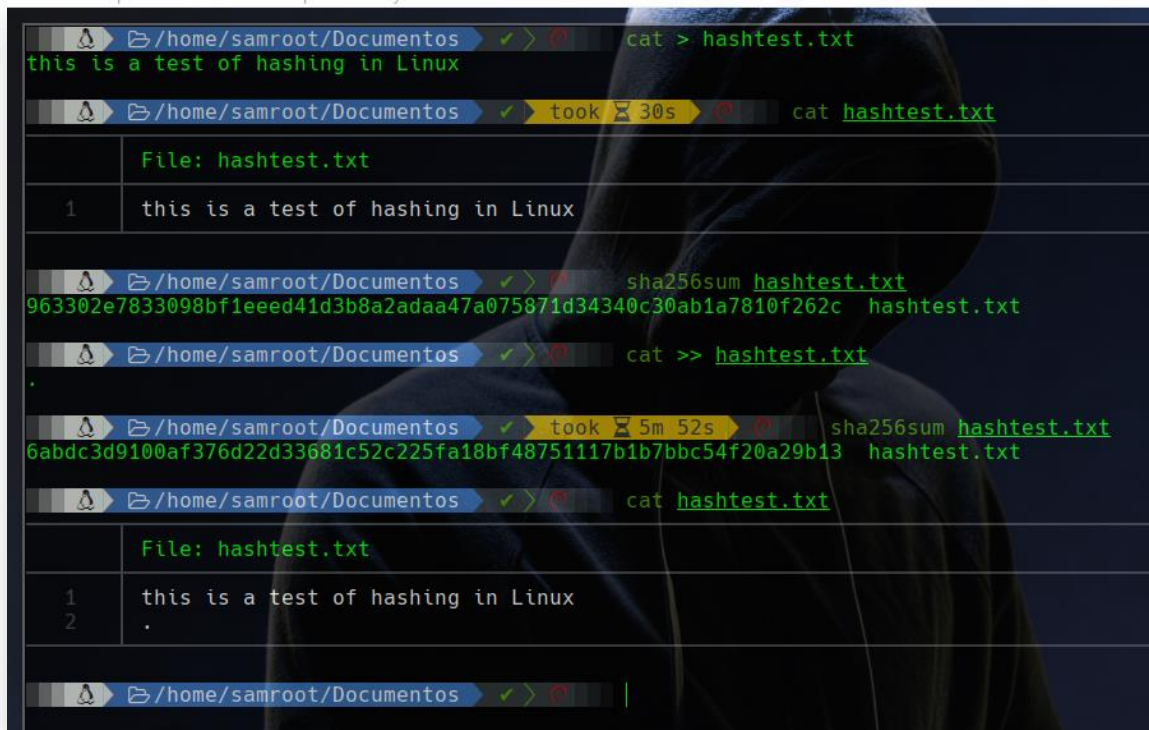


```
cat > hashtest.txt
this is a test of hashing in Linux
cat hashtest.txt
```

File: hashtest.txt	
1	this is a test of hashing in Linux

```
sha256sum hashtest.txt
963302e7833098bf1eed41d3b8a2adaa47a075871d34340c30ab1a7810f262c hashtest.txt
```

But let's add just a dot... nothing more... only a dot.



The screenshot shows a terminal window with the following commands and outputs:

```
/home/samroot/Documentos > cat > hashtest.txt
this is a test of hashing in Linux

/home/samroot/Documentos > cat hashtest.txt
File: hashtest.txt
1 this is a test of hashing in Linux

/home/samroot/Documentos > sha256sum hashtest.txt
963302e7833098bf1eed41d3b8a2adaa47a075871d34340c30ab1a7810f262c hashtest.txt

/home/samroot/Documentos > cat >> hashtest.txt
.

/home/samroot/Documentos > sha256sum hashtest.txt
6abdc3d9100af376d22d33681c52c225fa18bf48751117b1b7bbc54f20a29b13 hashtest.txt

/home/samroot/Documentos > cat hashtest.txt
File: hashtest.txt
1 this is a test of hashing in Linux
2 .
```

We can see that we only put an extra dot. And the output this time is a whole different string (hashvalue). that means that the data or the file has been altered or compromised.

Perhaps in our case we can decide not to use the compromised file and that would be all, but the hash has a very important relevance in the area of forensic computing since if the evidence has been altered or compromised, it will no longer be admissible in the investigation.

I hope you have learned something new. see you.