Forensic Investigation: Disk Drive Signature

October 20, 2020 By Raj Chandel

In this article, we will be using Disk Drive Signature to identify any suspicious changes in systems' directories or files. Creating such signatures can help us protect our data in various ways.

Table of Contents

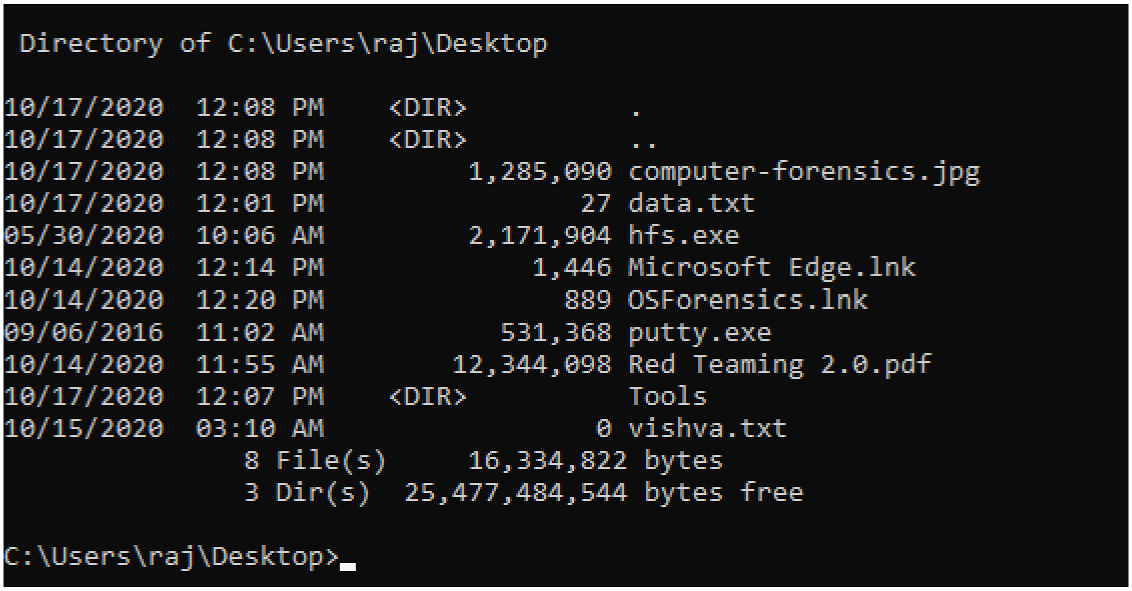
Introduction

A disk drive signature is created to identify the suspicious changes in your systems' directories or files. This data incorporates information about a document's path, size, and other file attributes.

To create a disk drive signature, we will be using the **OS Forensics** tool by PassMark Software. OS forensic allows you to create, compare, and analyse a disk drive signature.

Let's first check what all files are present there on the Desktop as we are going to create a disk signature on desktop only to get quick results. You can create a Disk drive Signature of any disk or folder present on your system as per your requirement.

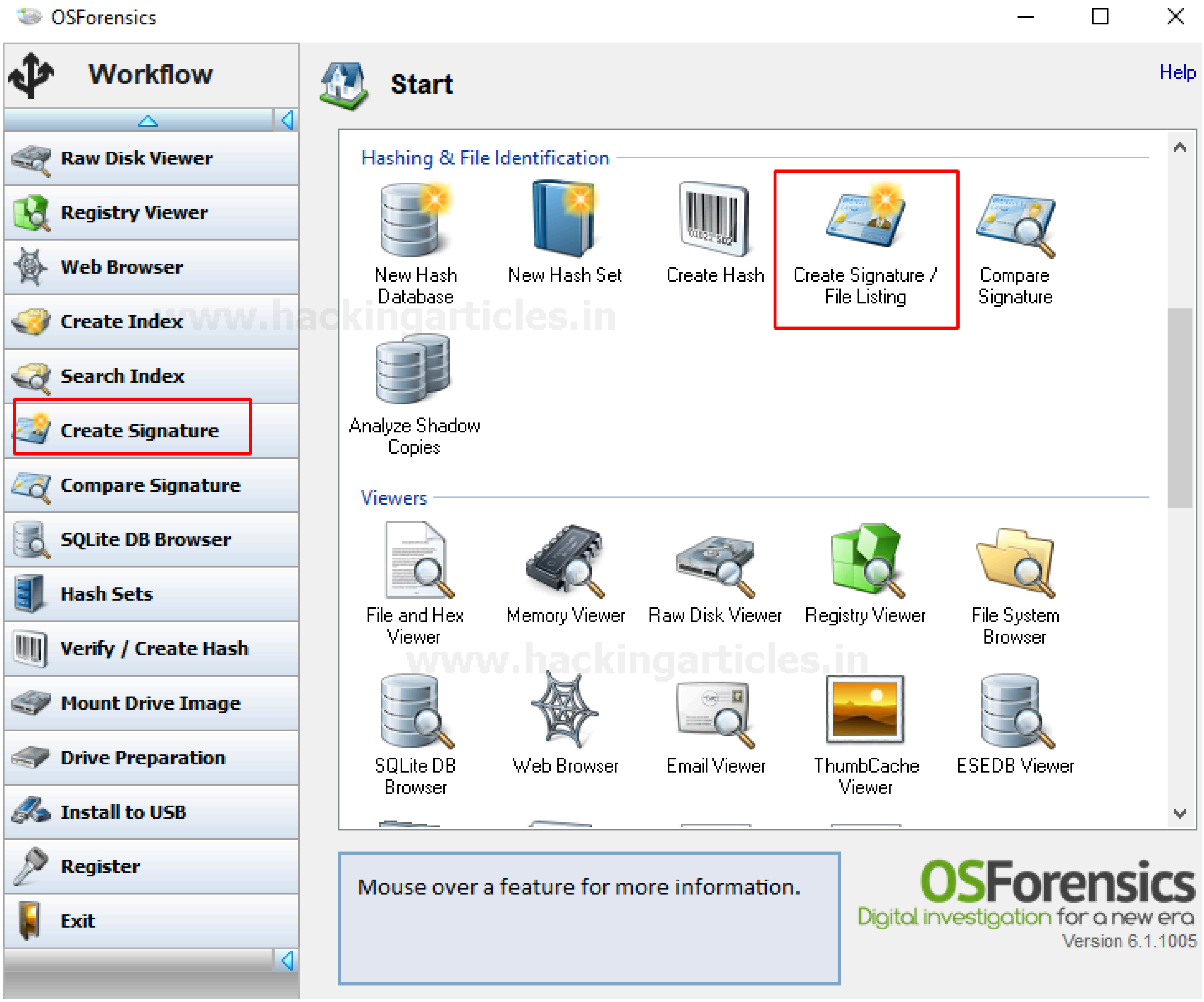
We are going to create a signature for my desktop only. To begin with let's first check the files present on the desktop so that you can get a clear idea after comparison of disk drive signatures.



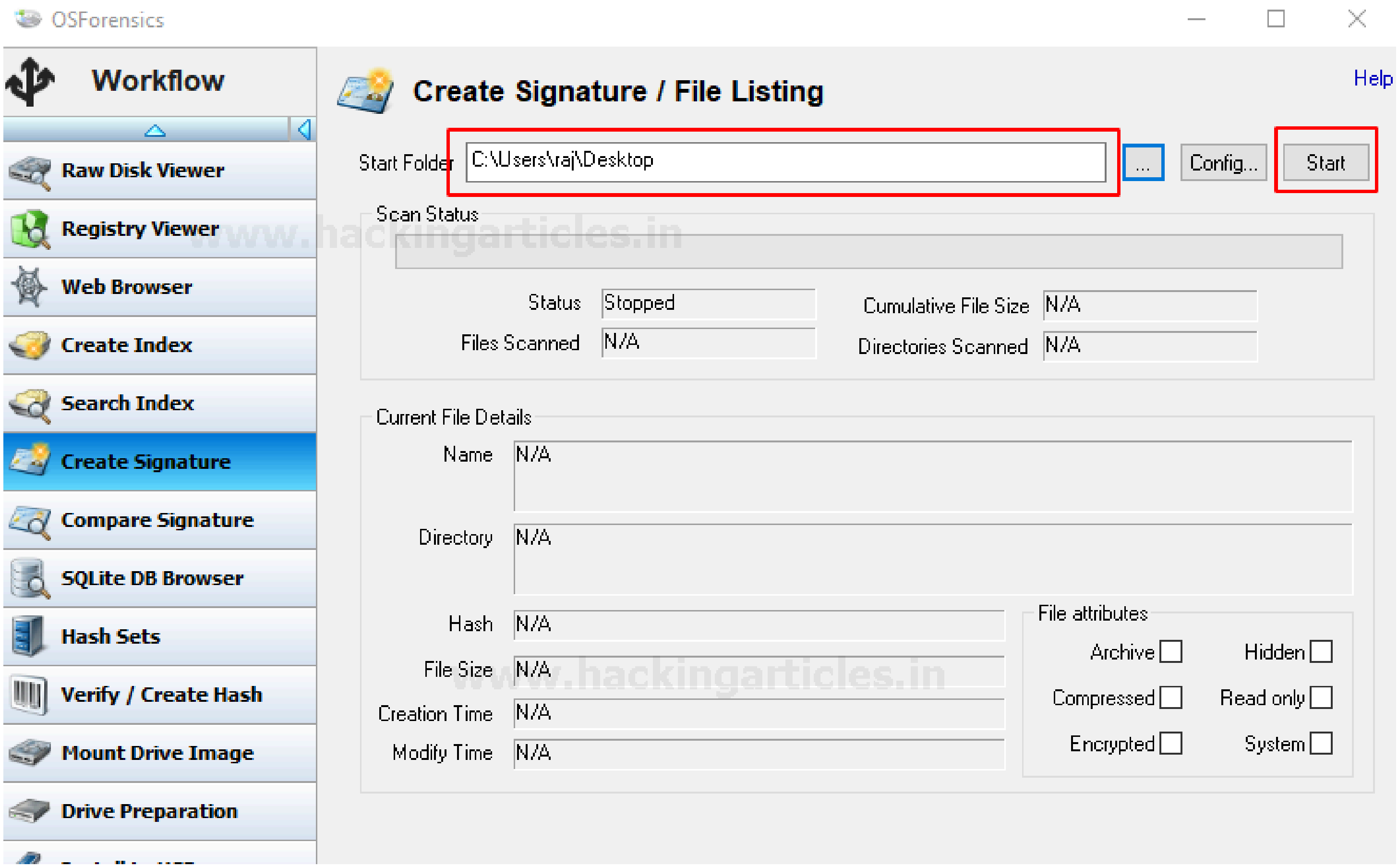
```
 Directory of C:\Users\raj\Desktop

10/17/2020  12:08 PM    <DIR>          .
10/17/2020  12:08 PM    <DIR>          ..
10/17/2020  12:08 PM         1,285,090 computer-forensics.jpg
10/17/2020  12:01 PM                27 data.txt
05/30/2020  10:06 AM         2,171,904 hfs.exe
10/14/2020  12:14 PM             1,446 Microsoft Edge.lnk
10/14/2020  12:20 PM               889 OSForensics.lnk
09/06/2016  11:02 AM           531,368 putty.exe
10/14/2020  11:55 AM        12,344,098 Red Teaming 2.0.pdf
10/17/2020  12:07 PM    <DIR>          Tools
10/15/2020  03:10 AM                 0 vishva.txt
               8 File(s)     16,334,822 bytes
               3 Dir(s)  25,477,484,544 bytes free

C:\Users\raj\Desktop>
```

Creating Disk Drive Signature

To create a Disk signature, download the OS Forensics tool if you haven't already. You can download it from **here**. You can create the disk signature by selecting the options highlighted in the following screenshot.



Select the desired directory to create the signature. Here, I have selected **Desktop**, browse the directory, and click start. So, the signature for the data drive will be created.



Start Folder: C:\Users\raj\Desktop

Scan Status

Status: Stopped
Cumulative File Size: N/A
Files Scanned: N/A
Directories Scanned: N/A

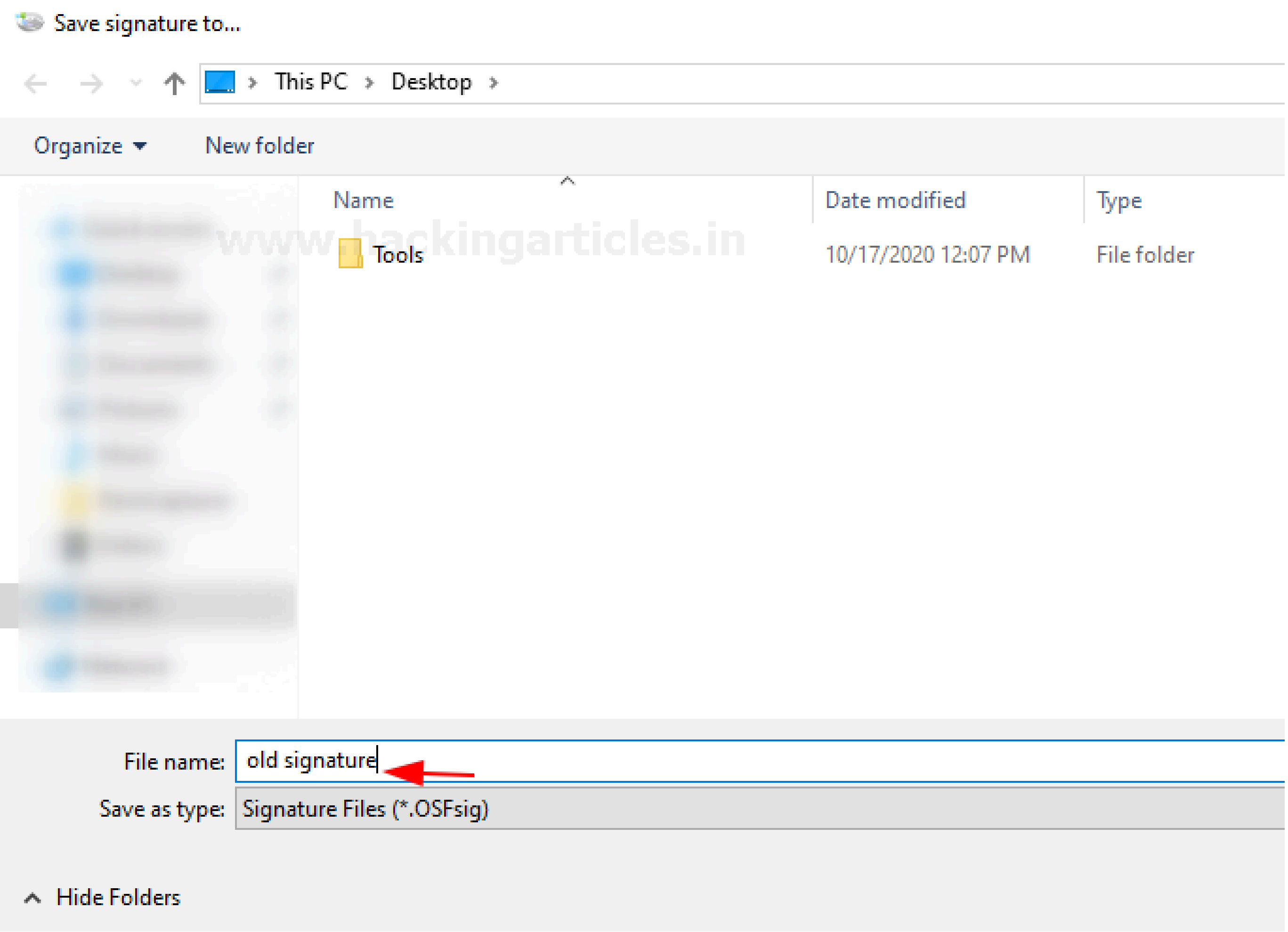
Current File Details

Name: N/A
Directory: N/A
Hash: N/A
File Size: N/A
Creation Time: N/A
Modify Time: N/A

File attributes

Archive □ Hidden □
Compressed □ Read only □
Encrypted □ System □

It will ask for the File Name, enter the File Name and click on Save. Now the signature for the selected drive will be created. Select a file name for your signature as per your convenience I will be naming the first signature “old signature” and the other one “new signature”, just to be clear while comparing both the signatures.

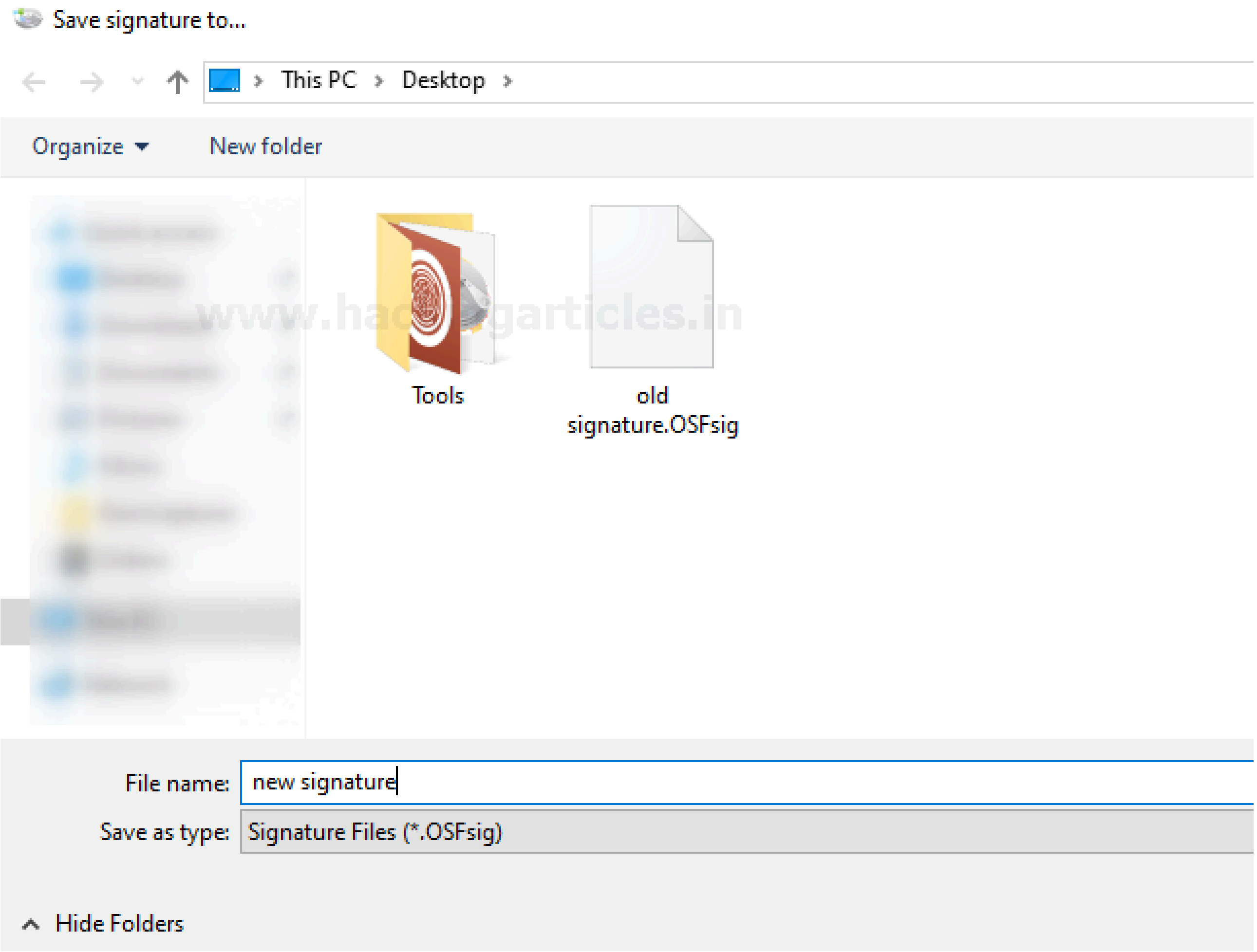


Name	Date modified	Type
Tools	10/17/2020 12:07 PM	File folder

File name: old signature

Save as type: Signature Files (*.OSFsig)

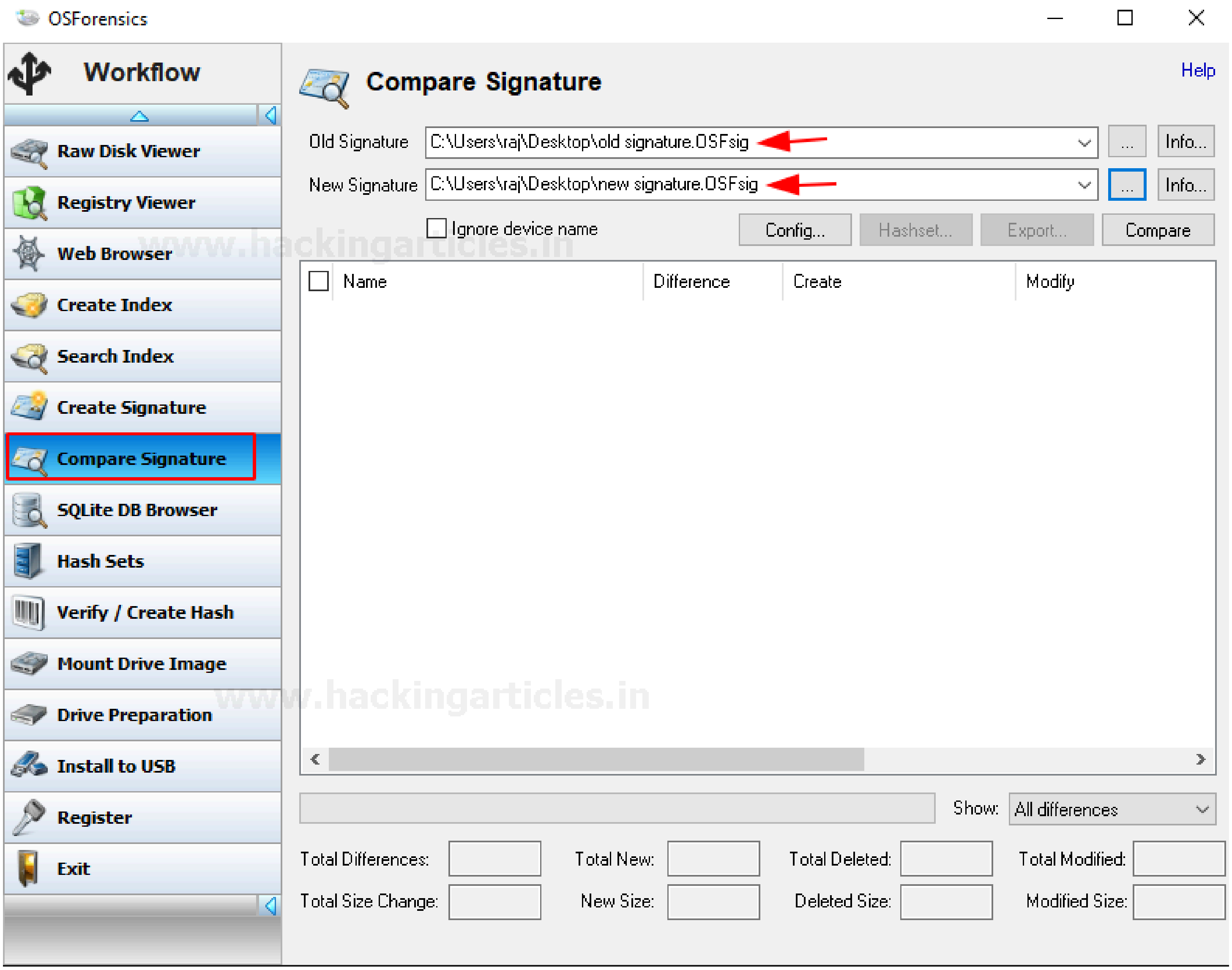
Now you can perform some modifications in the data drive like deleting or editing some files anything that you want. You can also repeat the same steps to create another signature after making all the alterations in the information drive.



File name: new signature

Save as type: Signature Files (*.OSFsig)

After creating the before and after signatures, select compare signature as highlighted in the following screenshot. Browse the old and new signature in the respective column and select **compare**. The comparison of the disk signature helps to find any changes in the drive.



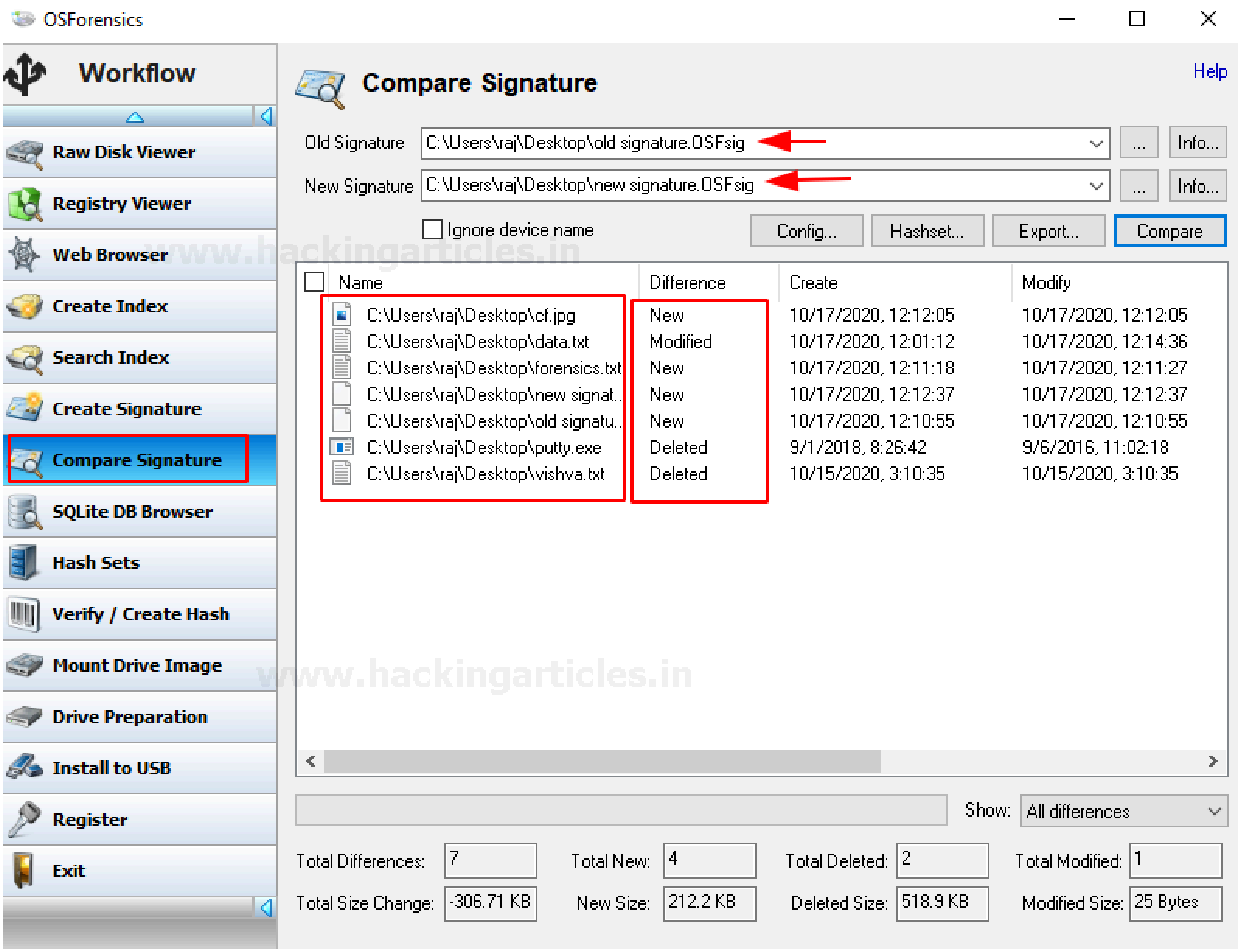
Old Signature: C:\Users\raj\Desktop\old signature.OSFsig

New Signature: C:\Users\raj\Desktop\new signature.OSFsig

□ Ignore device name

Show: All differences

The result will show the files with their difference status, whether the file is deleted, modified, or created along with the date and time. The result of after comparison of both the disk drive signature shows a total of 7 differences; 4 new files, 2 deleted, and 1 modified file.



Compare Signature

Old Signature: C:\Users\raj\Desktop\old signature.OSFsig

New Signature: C:\Users\raj\Desktop\new signature.OSFsig

□ Ignore device name

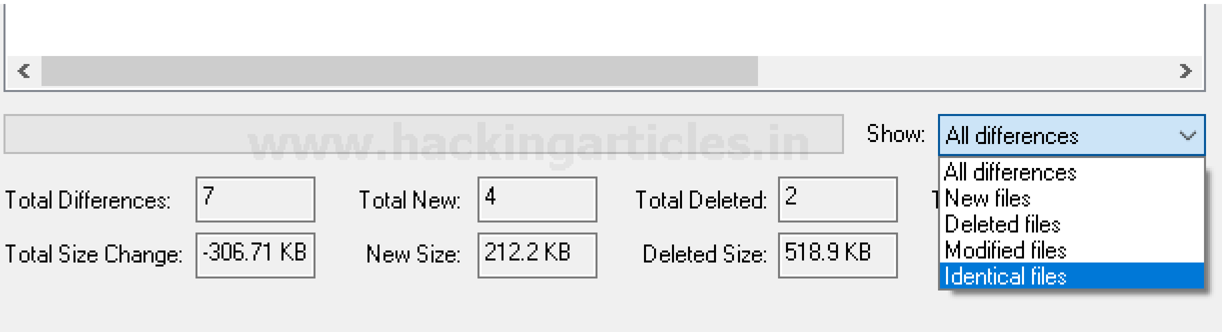
Name	Difference	Create	Modify
C:\Users\raj\Desktop\cf.jpg	New	10/17/2020, 12:12:05	10/17/2020, 12:12:05
C:\Users\raj\Desktop\data.txt	Modified	10/17/2020, 12:01:12	10/17/2020, 12:14:36
C:\Users\raj\Desktop\forensics.txt	New	10/17/2020, 12:11:18	10/17/2020, 12:11:27
C:\Users\raj\Desktop\new signat...	New	10/17/2020, 12:12:37	10/17/2020, 12:12:37
C:\Users\raj\Desktop\old signatu...	New	10/17/2020, 12:10:55	10/17/2020, 12:10:55
C:\Users\raj\Desktop\putty.exe	Deleted	9/1/2018, 8:26:42	9/6/2016, 11:02:18
C:\Users\raj\Desktop\vishva.txt	Deleted	10/15/2020, 3:10:35	10/15/2020, 3:10:35

Show: All differences

Total Differences: 7 Total New: 4 Total Deleted: 2 Total Modified: 1

Total Size Change: -306.71 KB New Size: 212.2 KB Deleted Size: 518.9 KB Modified Size: 25 Bytes

From the bottom right, as depicted in the picture, you can separately view the files of difference as you like. For instance, if you want to view all the deleted files altogether select deleted files from the drop-down column.



Show: All differences

Total Differences: 7 Total New: 4 Total Deleted: 2

Total Size Change: -306.71 KB New Size: 212.2 KB Deleted Size: 518.9 KB

Creating and comparing the disk drive signatures helps to know suspicious changes in your system as it creates a snapshot of the directory structure of the drive at the point of creation