

USB Forensics: Detection & Investigation

September 9, 2020 By Raj Chandel

Universal Serial Bus flash drives, commonly known as **USB flash drives** are the most common storage devices which can be found as evidence in Digital Forensics Investigation. The digital forensic investigation involves following a defined procedure for investigation which needs to be performed in such a manner that the evidence isn't destroyed. So, let us get started with the Forensics Investigation of USB.

Table of Contents

- **Detecting last attached USB flash drives in the Windows system**
- **Using Registry Editor**
- **Using PowerShell**
- **Using USBDeview**
- **Detecting last attached USB flash drives using Metasploit**
- **Investigating USB flash drives for deleted files**
- **Creating Disk Image**
- **Analysing Disk Image**

Detecting last attached USB flash drives in the Windows system

The usage of USB drives in place of work may let nasty employees remove sensitive or confidential information from a system without any authorization. To resolve this issue, forensic examination of systems comes into the picture. So, let's start investigating;

To detect the artifacts of the USB in the windows machine, we can use the manual as well as automated methods.

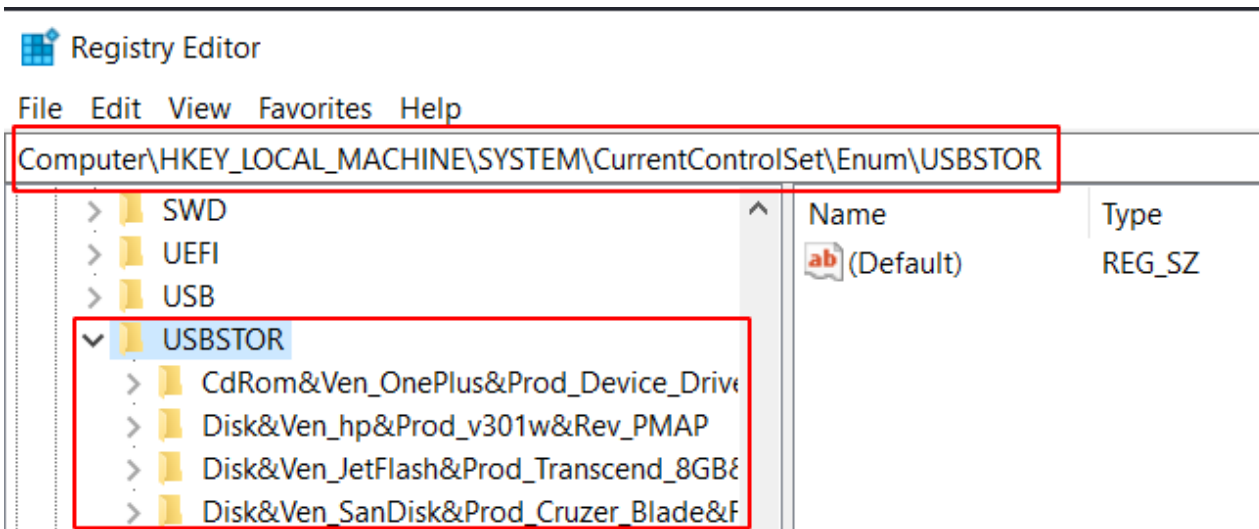
Using Registry Editor

It is a manual method to easily list the information of the last plugged in USB storage devices. Press '**Windows+R**' and type **Registry Editor**.

This information can be found in the Windows registry at:

```
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR
```

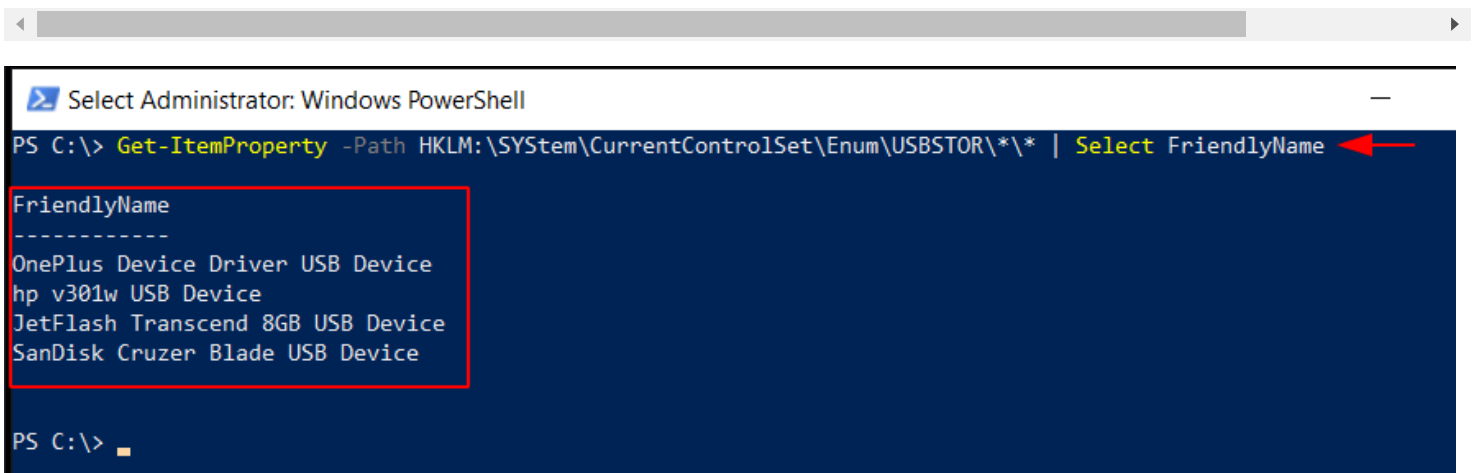
The details like last plugged in USB devices, the vendor of the USB, name of the product, serial number, and version name can be seen.



Using PowerShell

This is a manual method to find artifacts. The same path can be used in the PowerShell to get the information on last plugged in USB, with the following command;

```
Get-ItemProperty -Path HKLM:\System\CurrentControlSet\Enum\USBSTOR\*\* | Select-FriendlyName
```



Using USBDeview

To use an automatic method to find artifacts, you can download [USBDeview](#). This tool gives you an automated and a graphical representation understanding of what USB devices were connected to the system.

USBDeview

File Edit View Options Help

Description	Device Type	Connected	Safe To Unpl...	Disabled	USB Hub	Dr
Integrated Camera	Video	Yes	Yes	No	No	
ONEPLUS A6010	Unknown	No	Yes	No	No	
USB Mass Storage Device	Mass Storage	No	Yes	No	No	
USB Composite Device	Unknown	Yes	Yes	No	No	
USB Input Device	HID (Human Interface D...	Yes	Yes	No	No	
USB Input Device	HID (Human Interface D...	Yes	Yes	No	No	
USB Input Device	HID (Human Interface D...	Yes	Yes	No	No	
Goodix fingerprint SGX	Vendor Specific	Yes	Yes	No	No	
USB Composite Device	Unknown	Yes	Yes	No	No	
hp v301w USB Device	Unknown	No	Yes	No	No	E:
USB Composite Device	Unknown	No	Yes	No	No	
SanDisk Cruzer Blade USB Dev...	Mass Storage	No	Yes	No	No	
SanDisk Cruzer Blade USB Dev...	Unknown	No	Yes	No	No	
VMware USB Device	Unknown	No	Yes	No	No	
JetFlash Transcend 8GB USB D...	Unknown	No	Yes	No	No	G:
JetFlash Transcend 8GB USB D...	Mass Storage	No	Yes	No	No	G:
Intel(R) Wireless Bluetooth(R)	Bluetooth Device	Yes	Yes	No	No	
hp v301w USB Device	Mass Storage	Yes	Yes	No	No	E:

18 item(s), 1 Selected

NirSoft Freeware. <http://www.nirsoft.net> usb.ids is not loaded

Detecting last attached USB flash drives using Metasploit

When the USB flash drives history need to be investigated remotely, we can make use of modules in Metasploit in the Kali Linux. This module will enumerate USB Drive history on a target host. To use this module, switch on your Linux machine, start **msfconsole**, and type command;

```
use post/windows/gather/usb_history
```

Set the session number and exploit. Here you will be able to see a history of various USB connected previously.

```

msf5 > use post/windows/gather/usb_history
msf5 post(windows/gather/usb_history) > set session 1
session => 1
msf5 post(windows/gather/usb_history) > exploit

[*] Running module against STUPIDALIEN
[*]
J:          Disk 4f494d44
G:          Disk 3f005f
F:  SCSI#CdRom&Ven_Msft&Prod_Virtual_DVD-ROM#2&1f4adffe&0&000001#{53f5630d-b6bf-11d0-
[*] OnePlus Device Driver USB Device
=====
Disk lpftLastWriteTime      Unknown
Manufacturer               @cdrom.inf,%genmanufacturer%;(Standard CD-ROM drives)
Class
Driver                     {4d36e965-e325-11ce-bfc1-08002be10318}\0000
[*] hp v301w USB Device
=====
Disk lpftLastWriteTime      Unknown
Manufacturer               @disk.inf,%genmanufacturer%;(Standard disk drives)
Class
Driver                     {4d36e967-e325-11ce-bfc1-08002be10318}\0004
[*] JetFlash Transcend 8GB USB Device
=====
Disk lpftLastWriteTime      Unknown
Manufacturer               @disk.inf,%genmanufacturer%;(Standard disk drives)
Class
Driver                     {4d36e967-e325-11ce-bfc1-08002be10318}\0003
[*] SanDisk Cruzer Blade USB Device
=====
Disk lpftLastWriteTime      Unknown
Manufacturer               @disk.inf,%genmanufacturer%;(Standard disk drives)
Class
Driver                     {4d36e967-e325-11ce-bfc1-08002be10318}\0002
[*] Post module execution completed

```

Now you have also obtained the meterpreter session, so in order to use the powershell remotely to get the history of USB flash drives connected you can use the following command;

```
load powershell
```

Once the PowerShell is loaded, you can type,

```
Get-ItemProperty -Path HKLM:\SYStem\CurrentControlSet\Enum\USBSTOR\*\* | Select Fr
```

```
meterpreter > load powershell
Loading extension powershell ... Success.
meterpreter > powershell_shell
PS > Get-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Enum\USBSTOR\*\* | Select FriendlyName

FriendlyName
OnePlus Device Driver USB Device
hp v301w USB Device
JetFlash Transcend 8GB USB Device
SanDisk Cruzer Blade USB Device
```

You can hence see the list of USB Flash drives connected to the system remotely.

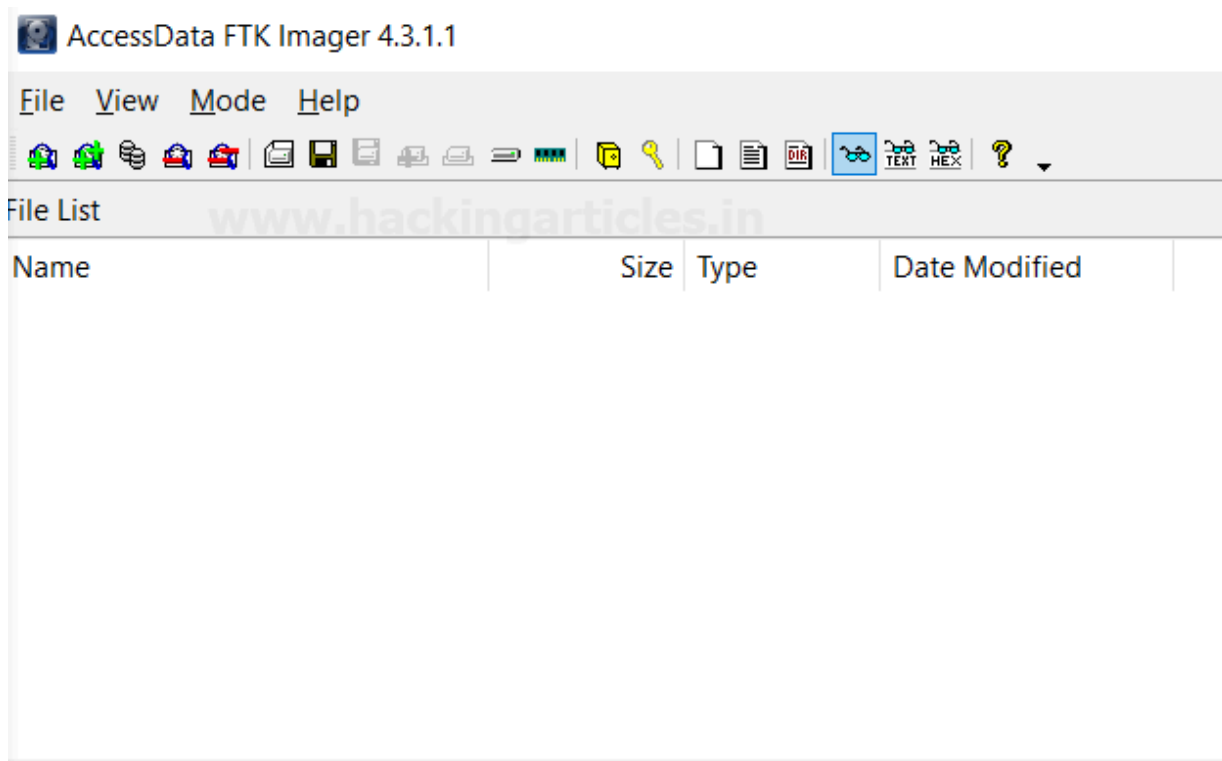
Investigating USB flash drives for deleted files.

After we have detected all the USB connection to the system and if the USB Flash drive is available at the scene of the crime. It can be carefully collected in **Faraday Bag** and now the forensic investigator can investigate the evidence.

At first, it is important to create an image of the USB flash drive that was retrieved from the crime scene. To create an image and to analyse, we can use **FTK® Imager**, which can be downloaded from [here](#).

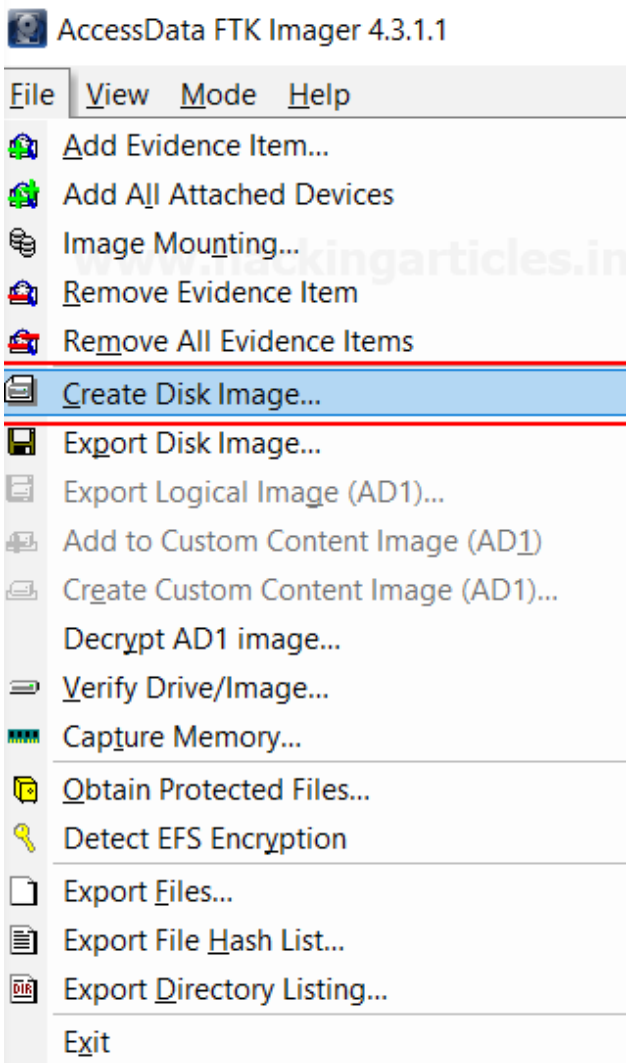
Creating Disk Image

Step 1: Install and run AccessData FTK imager

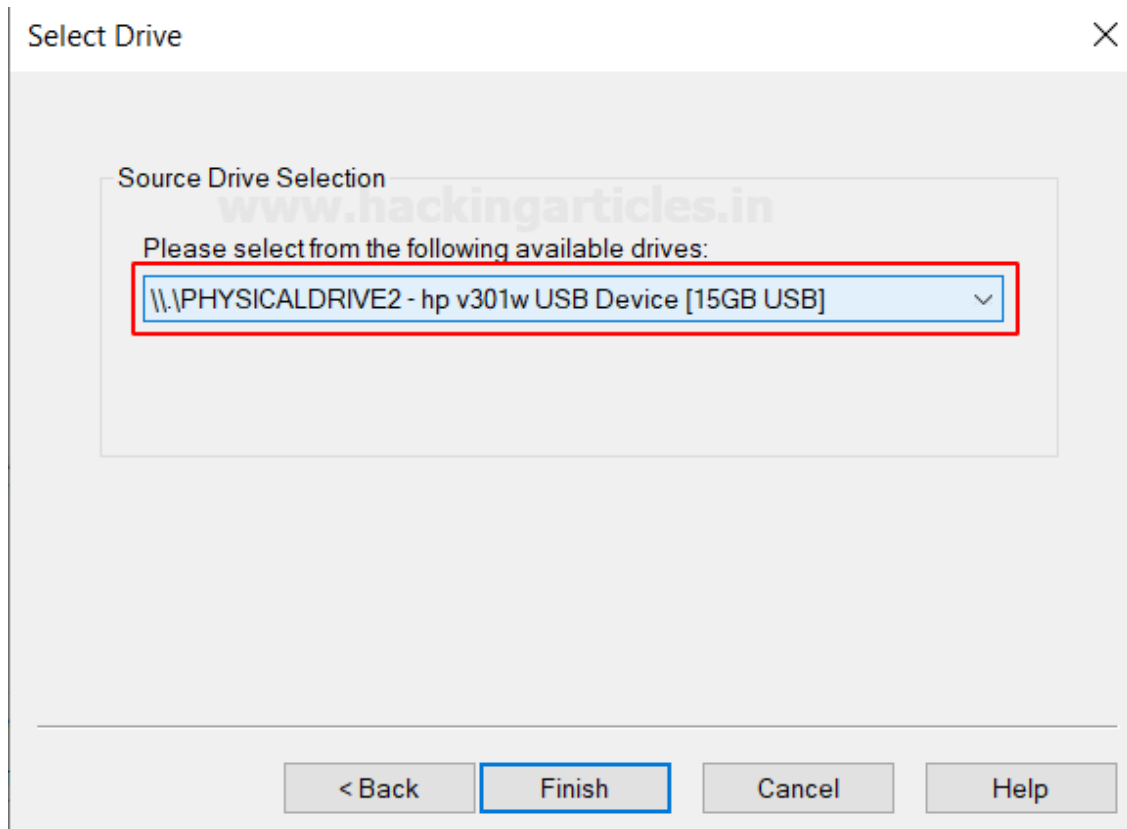
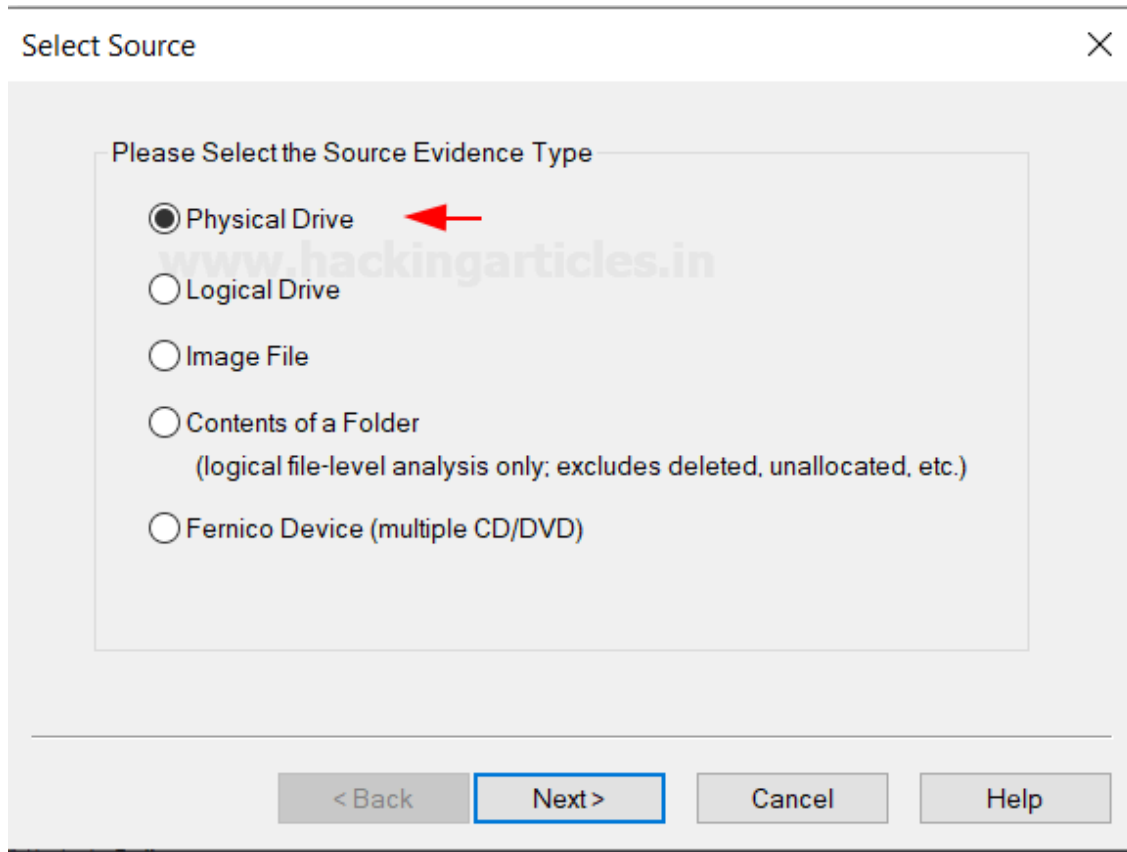


Step 2. Create a disk image of the USB Drive

A **disk image** is a bit-by-bit or a sector-by-sector copy of a physical storage device like USB Flash drive, which includes all files, folders and unallocated, free and slack space etc.



Step 3: As it as USB Flash drive, select Physical Drive and its source to create an image and click on finish.



Step 4: Add the destination of the image file, check the box which say verify images that are created.

Create Image ×

Image Source

\\.\PHYSICALDRIVE2

Starting Evidence Number: 1

Image Destination(s)

Add... Edit... Remove

Add Overflow Location

☒ Verify images after they are created ☐ Precalculate Progress Statistics

☐ Create directory listings of all files in the image after they are created

Start Cancel

Step 5: After adding the destination of the image file to be created, type the name you want to give to the image file and click on finish.

Select Image Destination ×

Image Destination Folder

J:\ Browse

Image Filename (Excluding Extension)

USBForensics

Image Fragment Size (MB) 1500

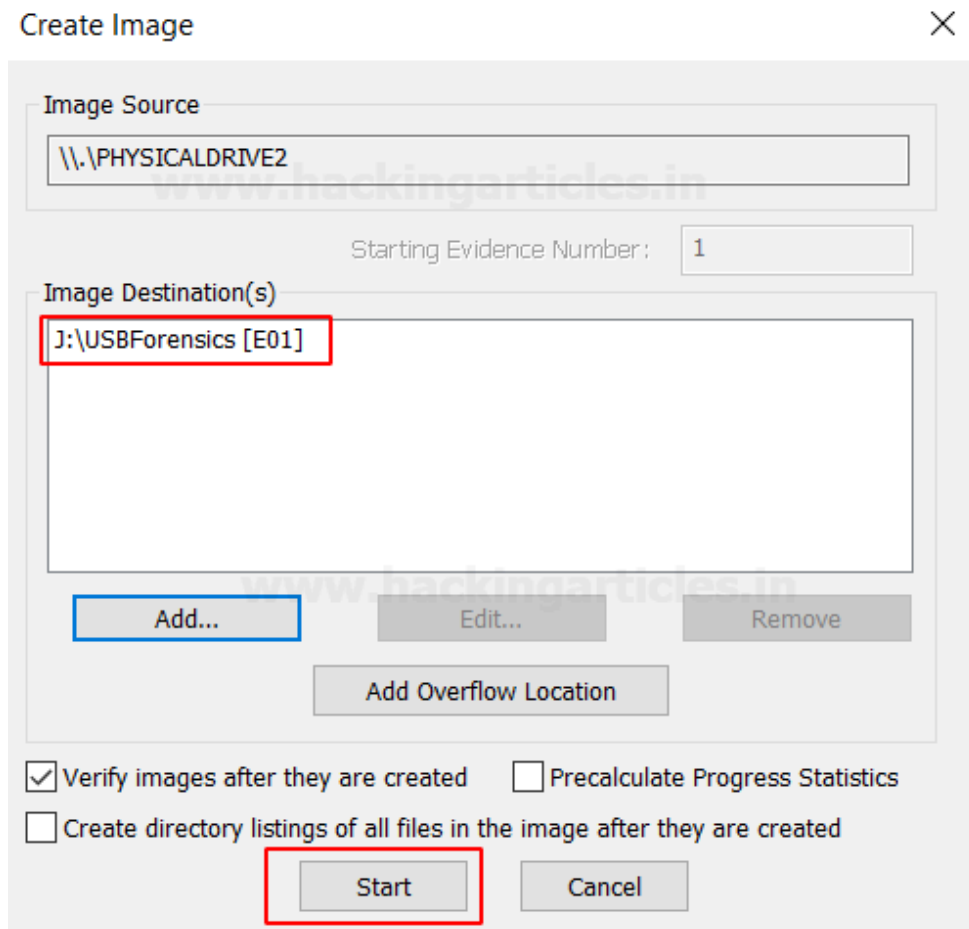
For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest) 6

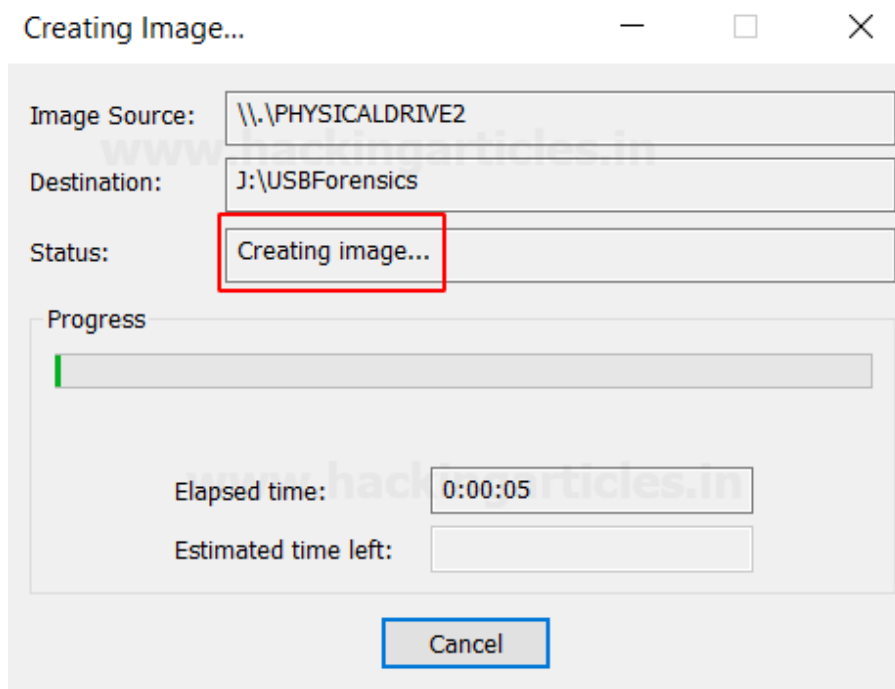
Use AD Encryption ☐

< Back Finish Cancel Help

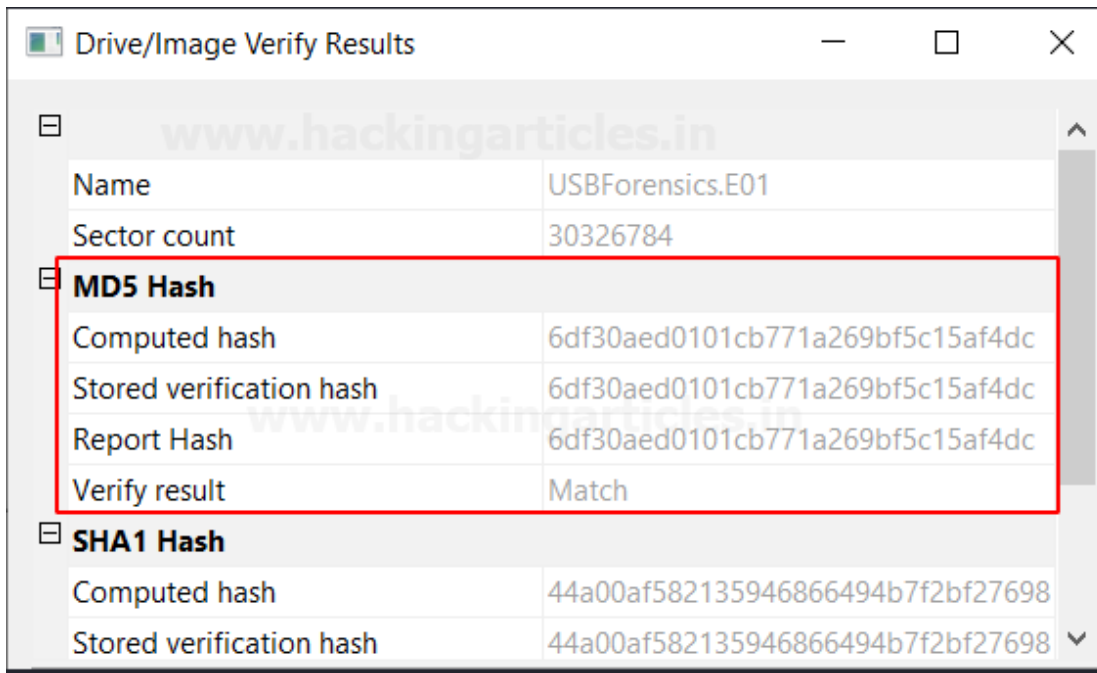
Step 6: You can see that the image destination is ready, then click on Start to begin imaging.



Step 7: You see that the image of your USB flash Drive is being created.



Step 8: After the imaging is completed, you will be prompted with MD% image verification details where a compared and verified hash is generated.



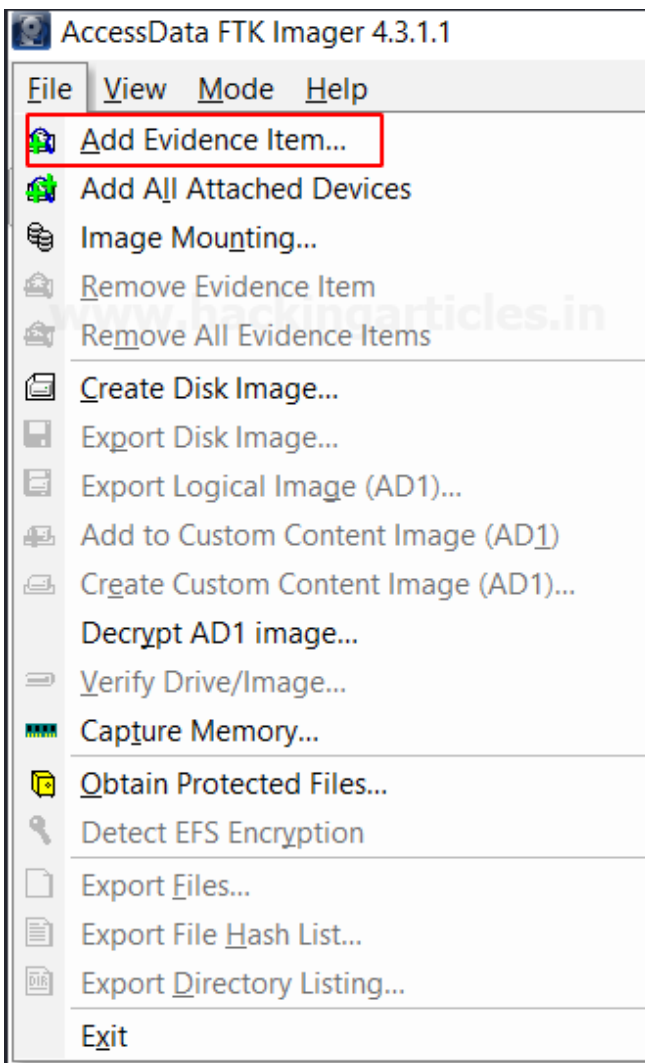
Drive/Image Verify Results	
www.hackingarticles.in	
Name	USBForensics.E01
Sector count	30326784
MD5 Hash	
Computed hash	6df30aed0101cb771a269bf5c15af4dc
Stored verification hash	6df30aed0101cb771a269bf5c15af4dc
Report Hash	6df30aed0101cb771a269bf5c15af4dc
Verify result	Match
SHA1 Hash	
Computed hash	44a00af582135946866494b7f2bf27698
Stored verification hash	44a00af582135946866494b7f2bf27698

Here the imaging part is over, so we can now move to the analysis of the USB Flash Drive.

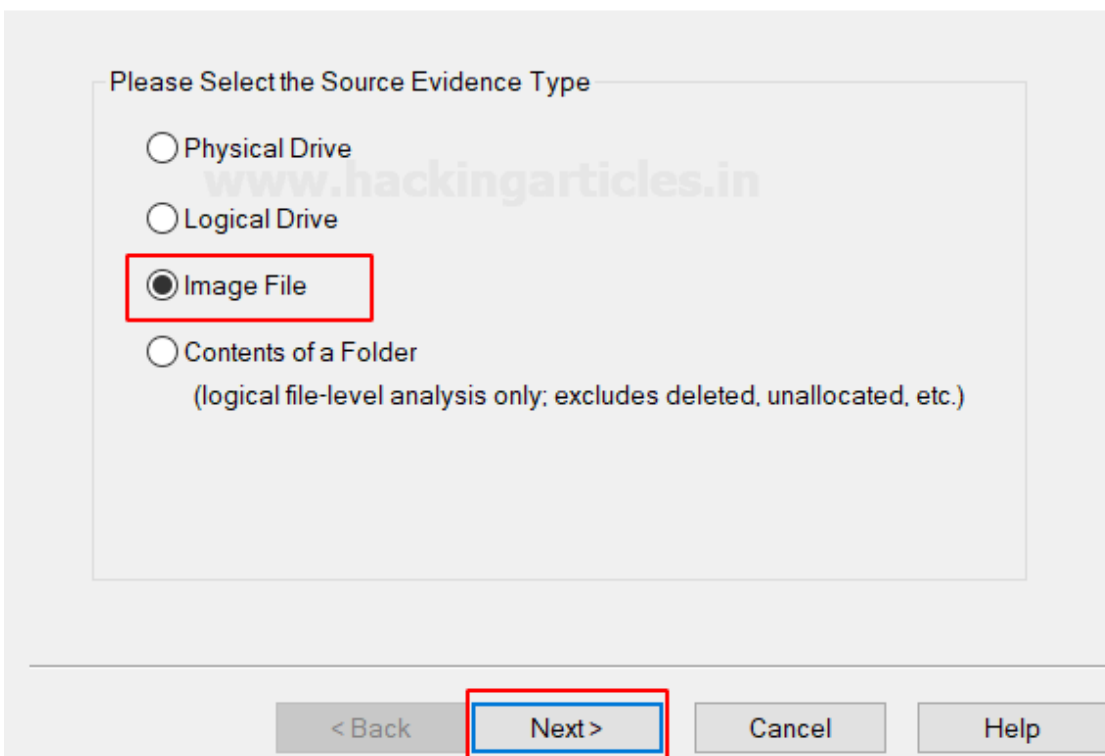
Analysing Disk Image

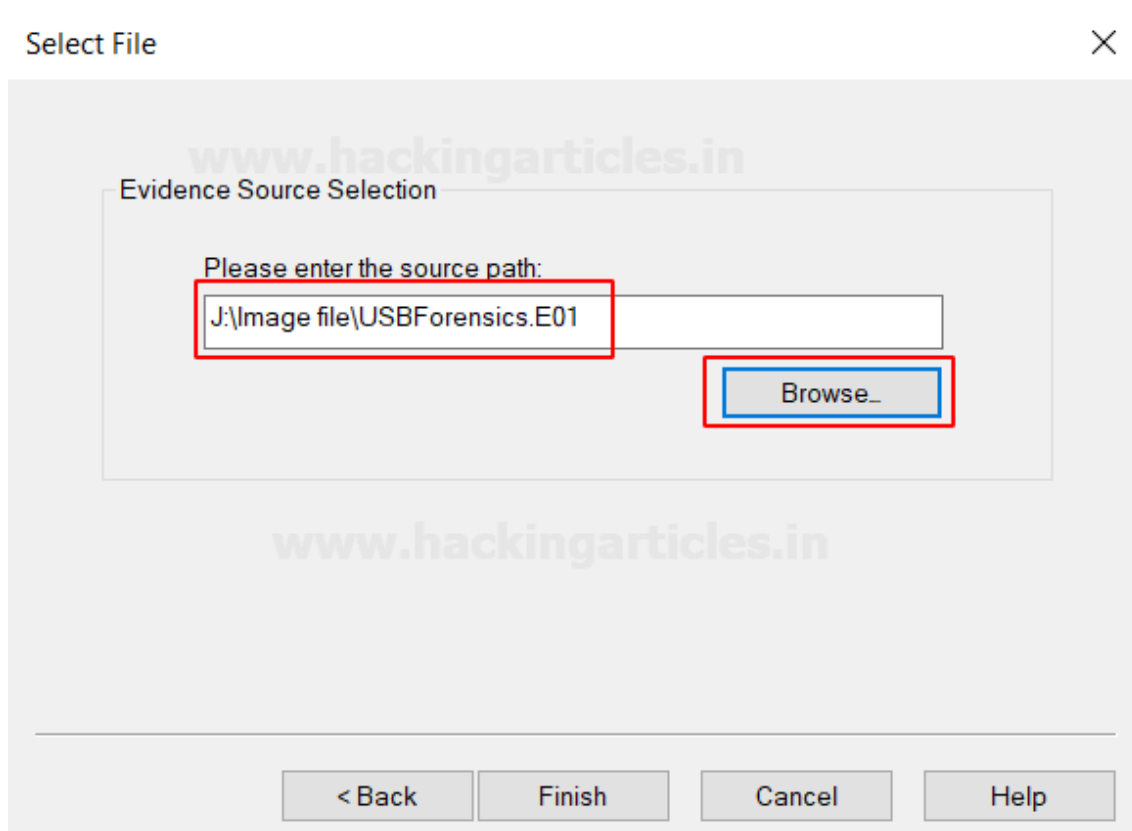
Note: Investigation is to be performed only on the Disk image of the original evidence.

Step 9: Click on add evidence item and add the source of the created image file.

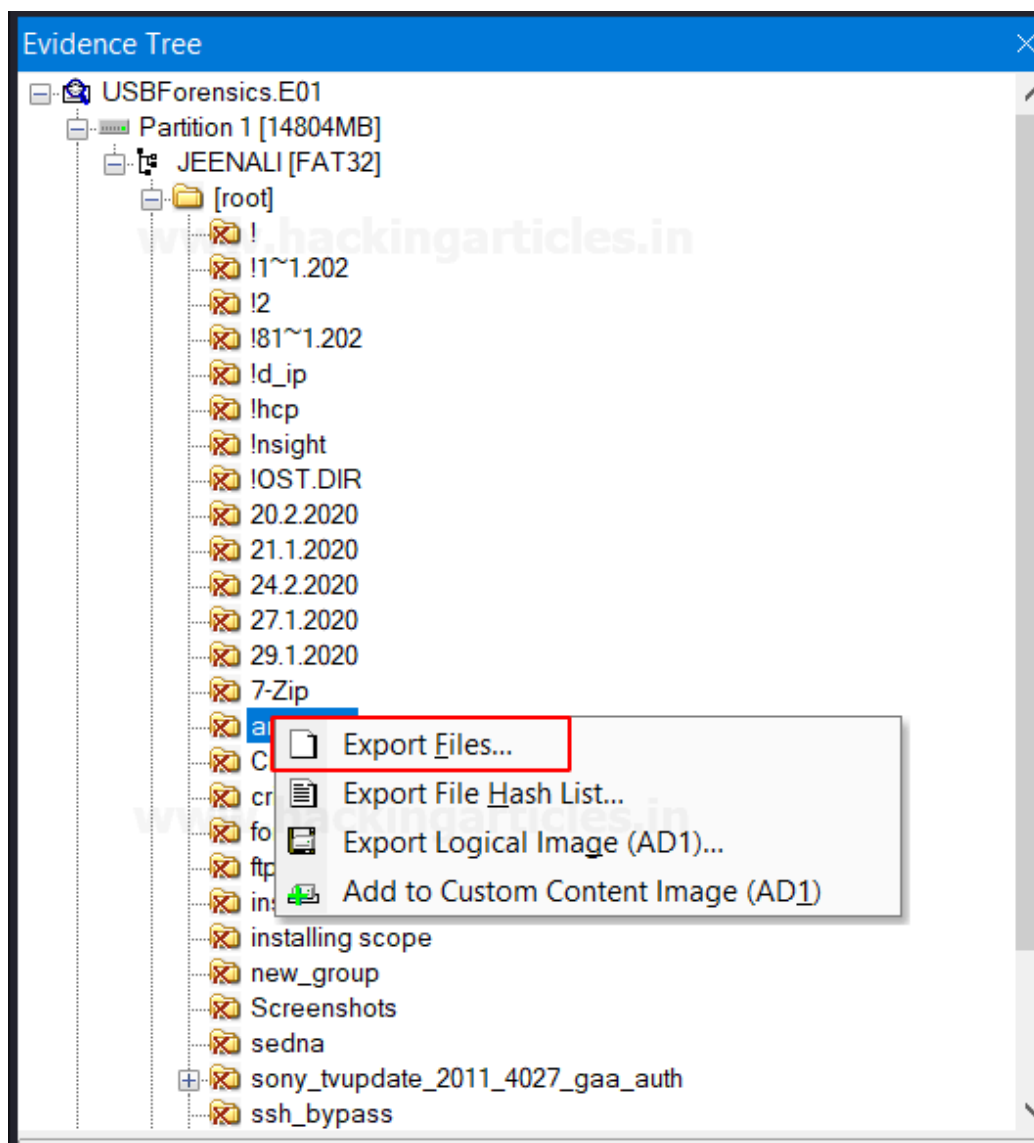


Select Source





Step 10: Here you see that an evidence tree is created and the root folder has deleted folders. Here we will try to retrieve them by clicking on 'Export files'



Step 11: You see that the deleted folder and the contents of the deleted folder have been retrieved.

armitage



Search armitage



armitage