Multiple Ways to Create Image file for Forensics Investigation

January 1, 2020 By Raj Chandel

In this article, we will learn how to capture the forensic image of the victim's hard drives and systems to get help in the investigation. There are multiple ways to do that work and these tools will help us a lot in the process of an investigation so let's start this process.

Table of Content

Introduction

In today's digital era, the indulgence of devices is increasing more and more and with-it cybercrime is also on the rise. When such a crime occurs, the hard drive becomes an important part as it is crucial evidence. Therefore, during investigation one cannot directly perform various tasks on the hard drive as it is considered tempered. Also, one can lose data by mistake while performing tasks on it. Hence, the necessity of disk image. Now that we have understood the importance and use of disk image, let us now understand that what exactly a forensic image is.

What is a Forensic image?

A Forensic image is an exact copy of hard drive. This image is created using various third-party tools which can easily capture the image of a hard drive bit by bit without changing even a shred of data. Forensic software copies data by creating a bitstream which is an exact duplicate. The best thing about creating a forensic image is that it also copies the deleted data, including files that are left behind in swap and free spaces. Now that we have understood all about the forensic imaging, let us now focus on the practical side of it. We will learn and understand how to create such image by using five different tools which are:

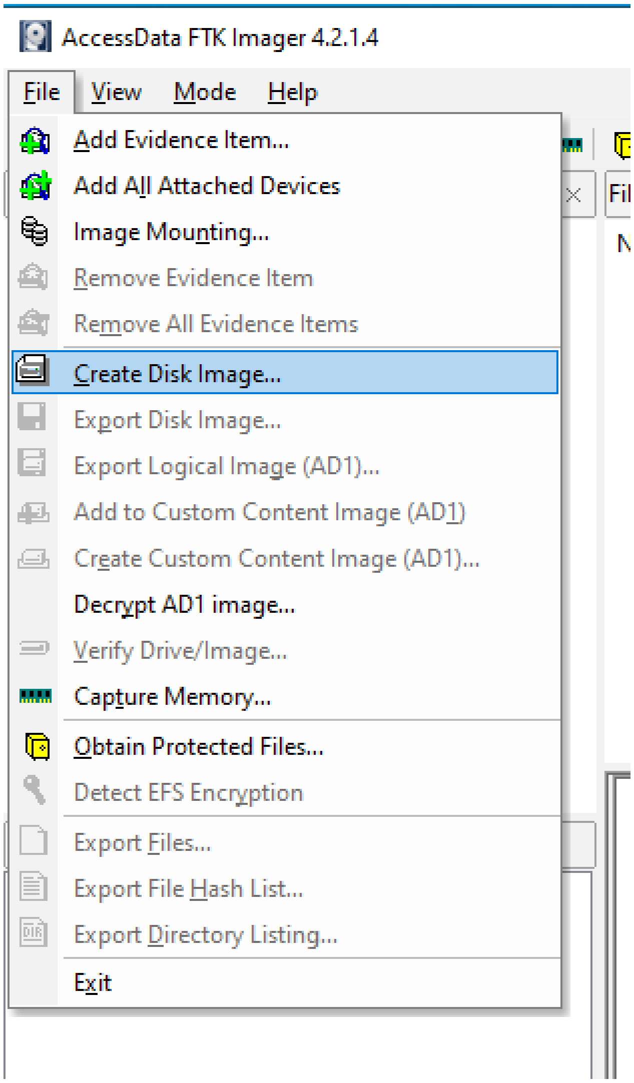
1. FTK Imager
2. Belkasoft acquisition tool
3. Encase imager
4. Forensic imager

FTK Imager

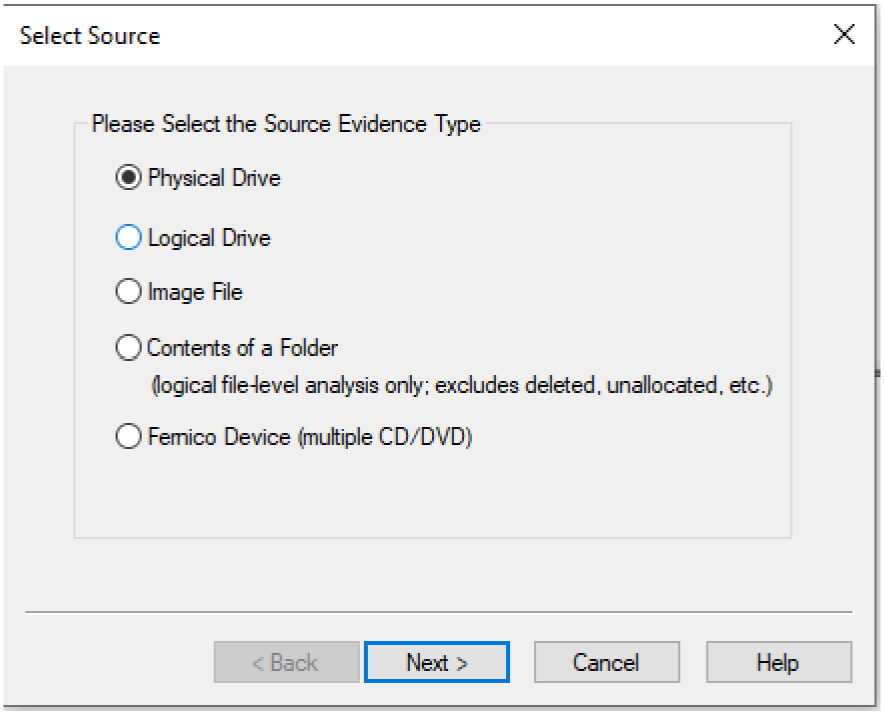
FTK imager can create an image and paging file for windows; along with capturing volatile memory for analysis purpose.

We can download FTK imager from **here**

After installing the FTK imager we can start by creating an image and to do so, we have to go to the file button and from the drop-down menu, select the Create Disk Image option.



After selecting the create disk image it will ask you the evidence type whether i.e. physical drive, logical drive, etc. and once you have selected the evidence type then press the next button to move further in the process.



Please Select the Source Evidence Type

● Physical Drive

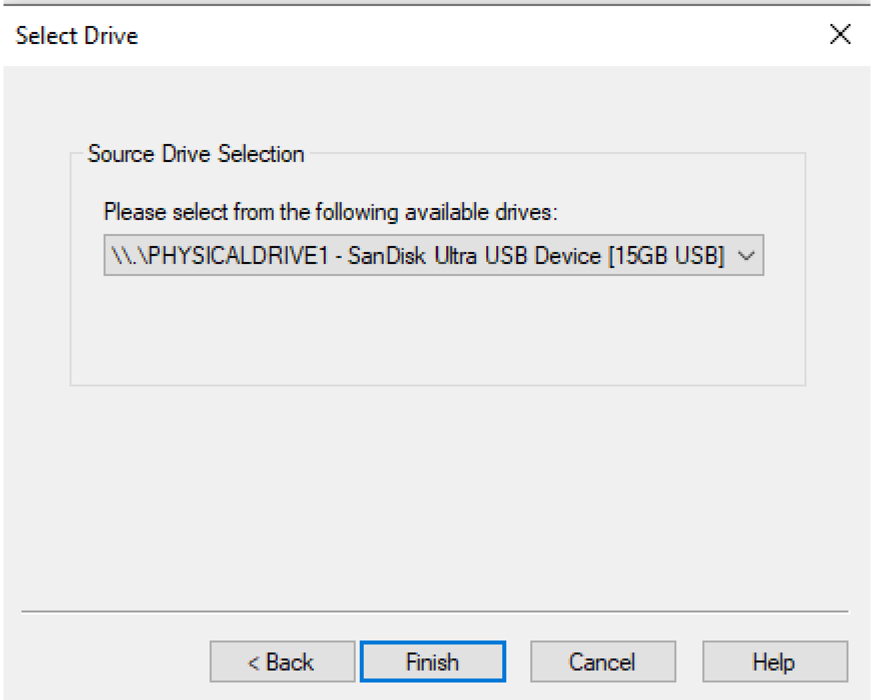
○ Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Femico Device (multiple CD/DVD)

Now it will ask for the drive of which you want to create the image. Select that drive and click on Finish button.

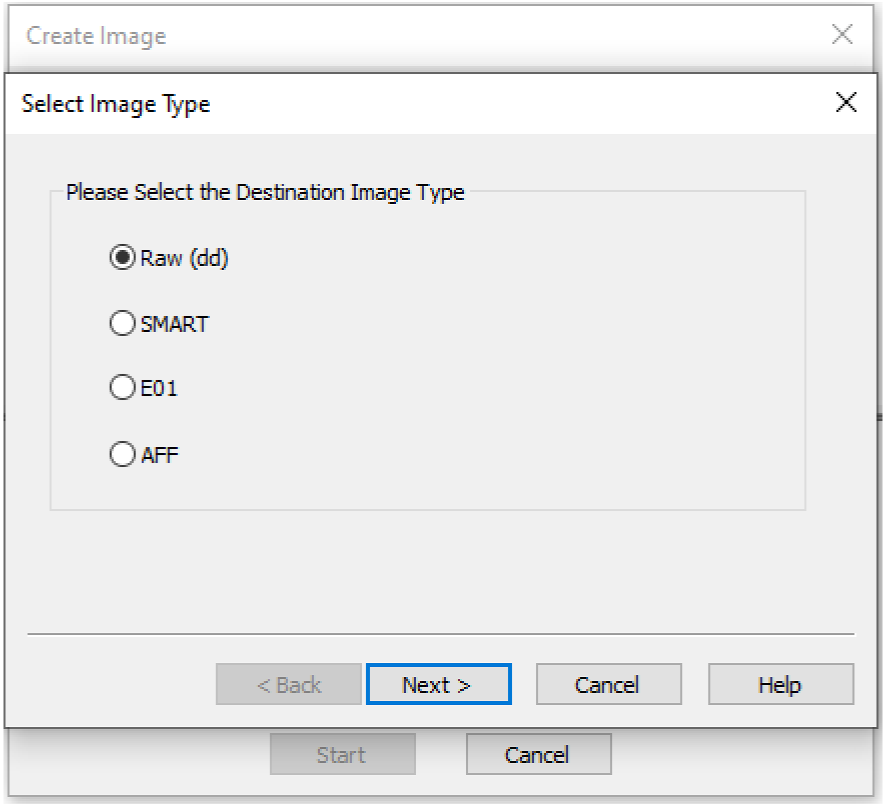


Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE1 - SanDisk Ultra USB Device [15GB USB]

Now, we need to provide the image destination i.e. where we want our image to be saved. And to give the path for the destination, click on Add button.



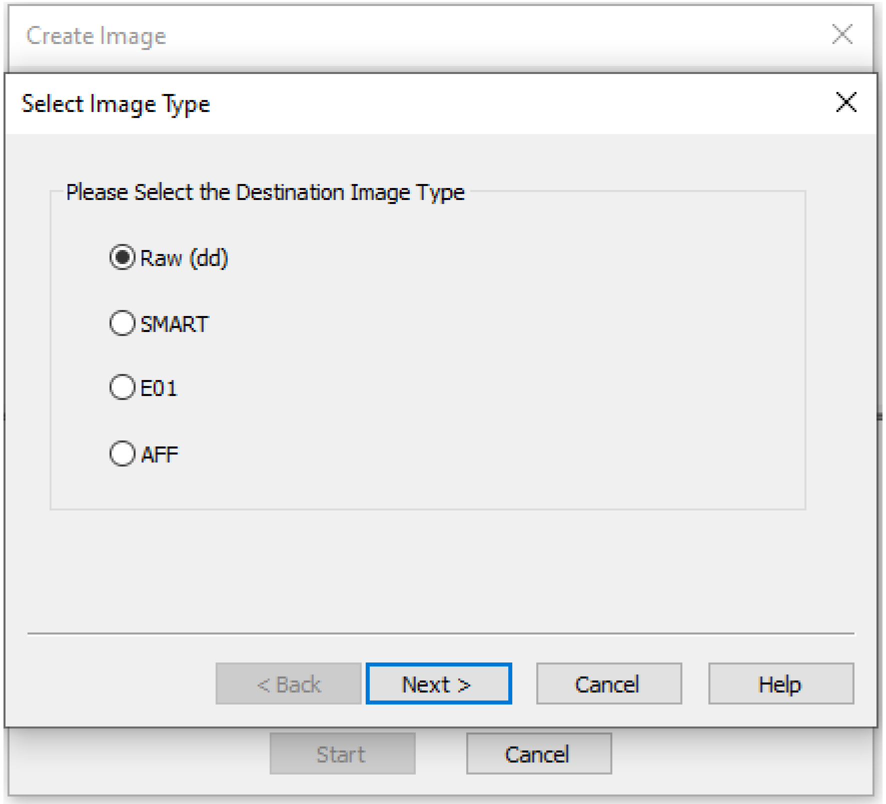
Create Image

Select Image Type

Please Select the Destination Image Type

- ● Raw (dd)
- ○ SMART
- ○ E01
- ○ AFF

Then select the type you want your image to be i.e. raw or E01, etc. Then click on Next button.



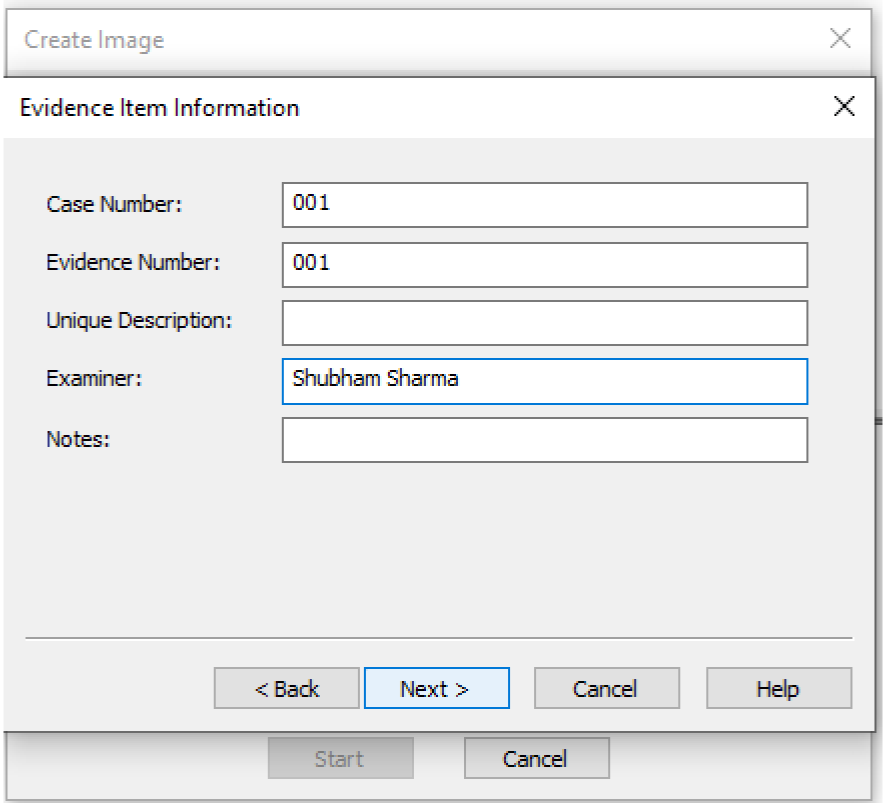
Create Image

Select Image Type

Please Select the Destination Image Type

- ● Raw (dd)
- ○ SMART
- ○ E01
- ○ AFF

Further it will ask you to provide details for the image such as case number, evidence number, unique description, examiner, notes about the evidence or investigation. Click on Next button after providing all the details.



Case Number: 001

Evidence Number: 001

Unique Description:

Examiner: Shubham Sharma

Notes:

After this, it will ask you for the destination folder i.e. where you want your image to be saved along with its name and fragment size. Once you fill up all the details, click on the Finish button.

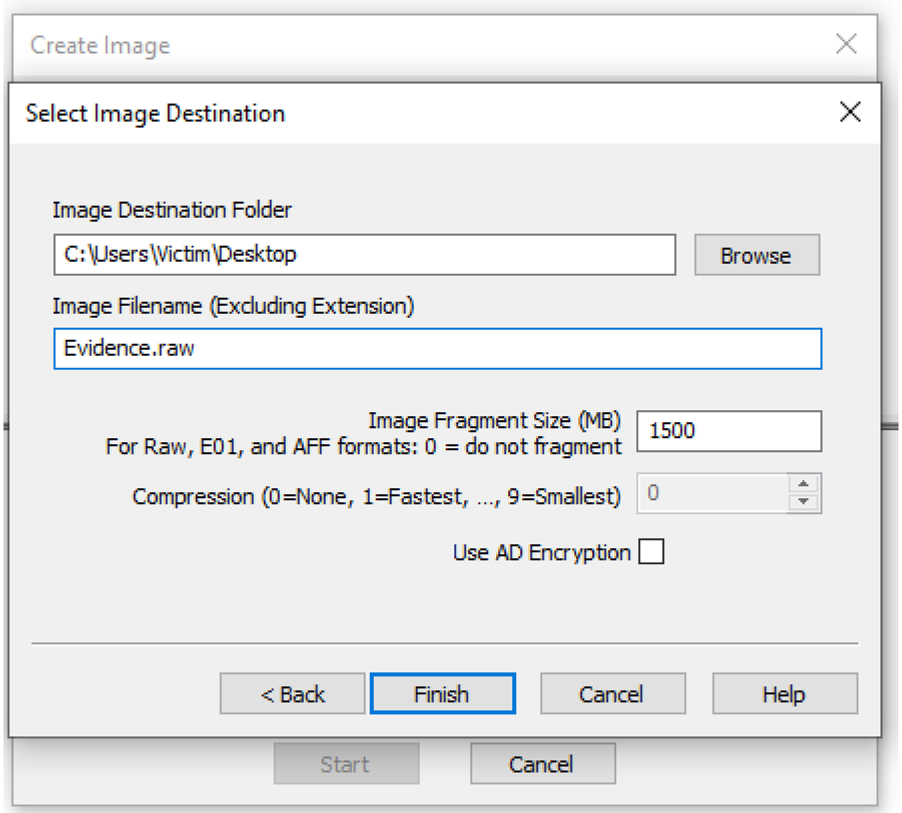


Image Destination Folder: C:\Users\Victim\Desktop

Image Filename (Excluding Extension): Evidence.raw

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 1500

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

Use AD Encryption □

And now the process to create the image will start and it will simultaneously inform you about the elapsed time, estimated time left, image source, destination and status.

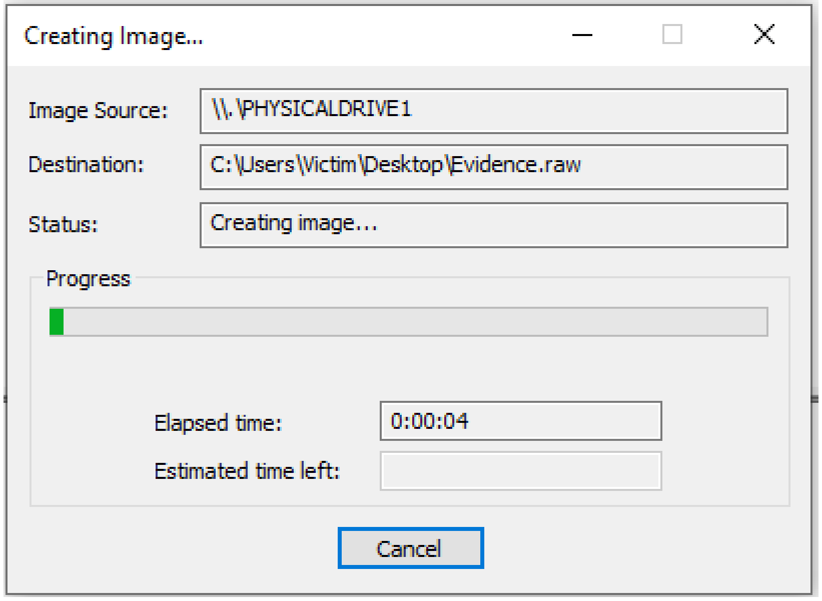

Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Users\Victim\Desktop\Evidence.raw

Status: Creating image...

Elapsed time: 0:00:04

Estimated time left:

After the progress bar completes and status shows Image created successfully then it means our forensic image is created successfully .

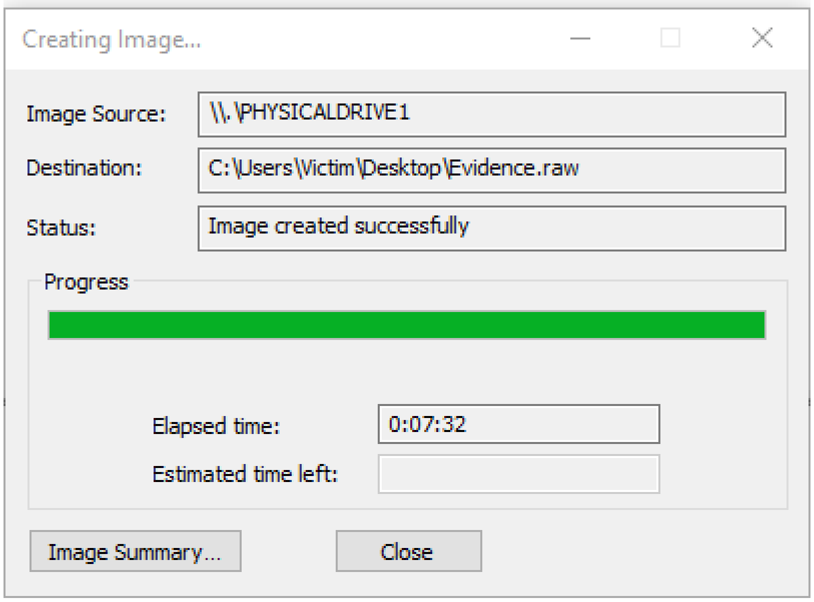

Creating Image...

Image Source: \\.\PHYSICALDRIVE1

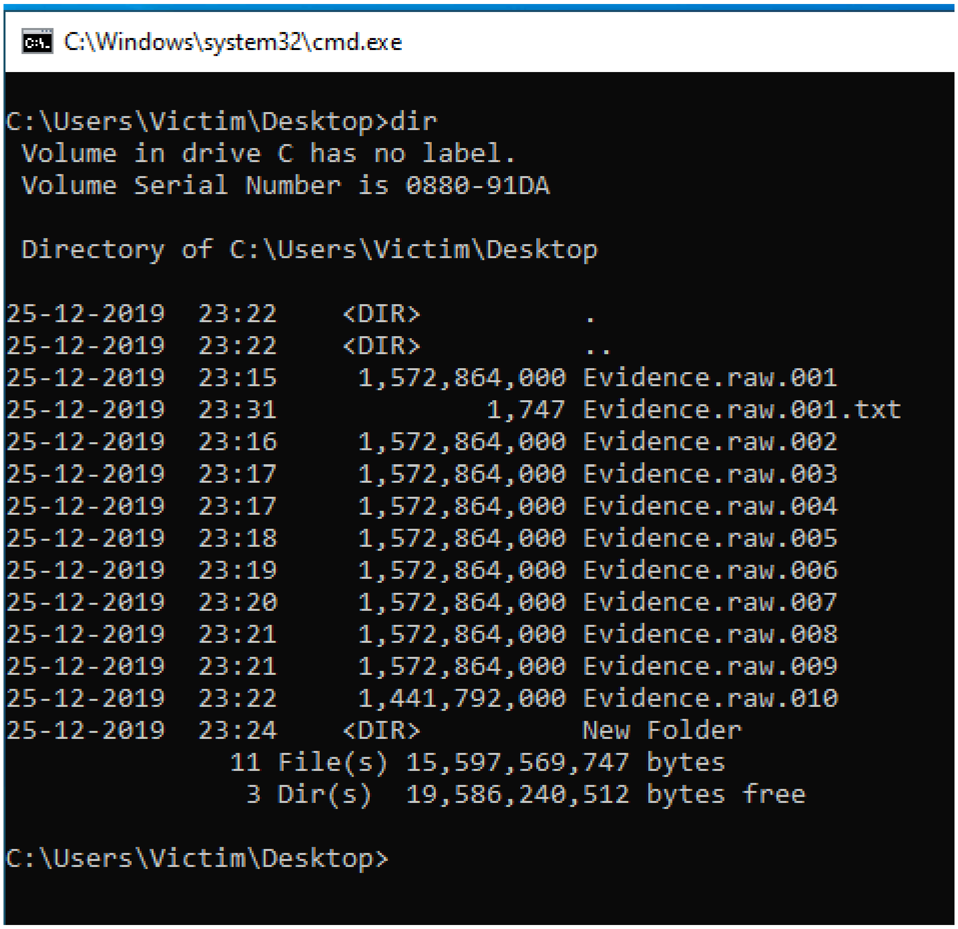
Destination: C:\Users\Victim\Desktop\Evidence.raw

Status: Image created successfully

Elapsed time: 0:07:32

Estimated time left:

And so, after the creation of the image you can go to the destination folder and verify the image as shown in the picture below :



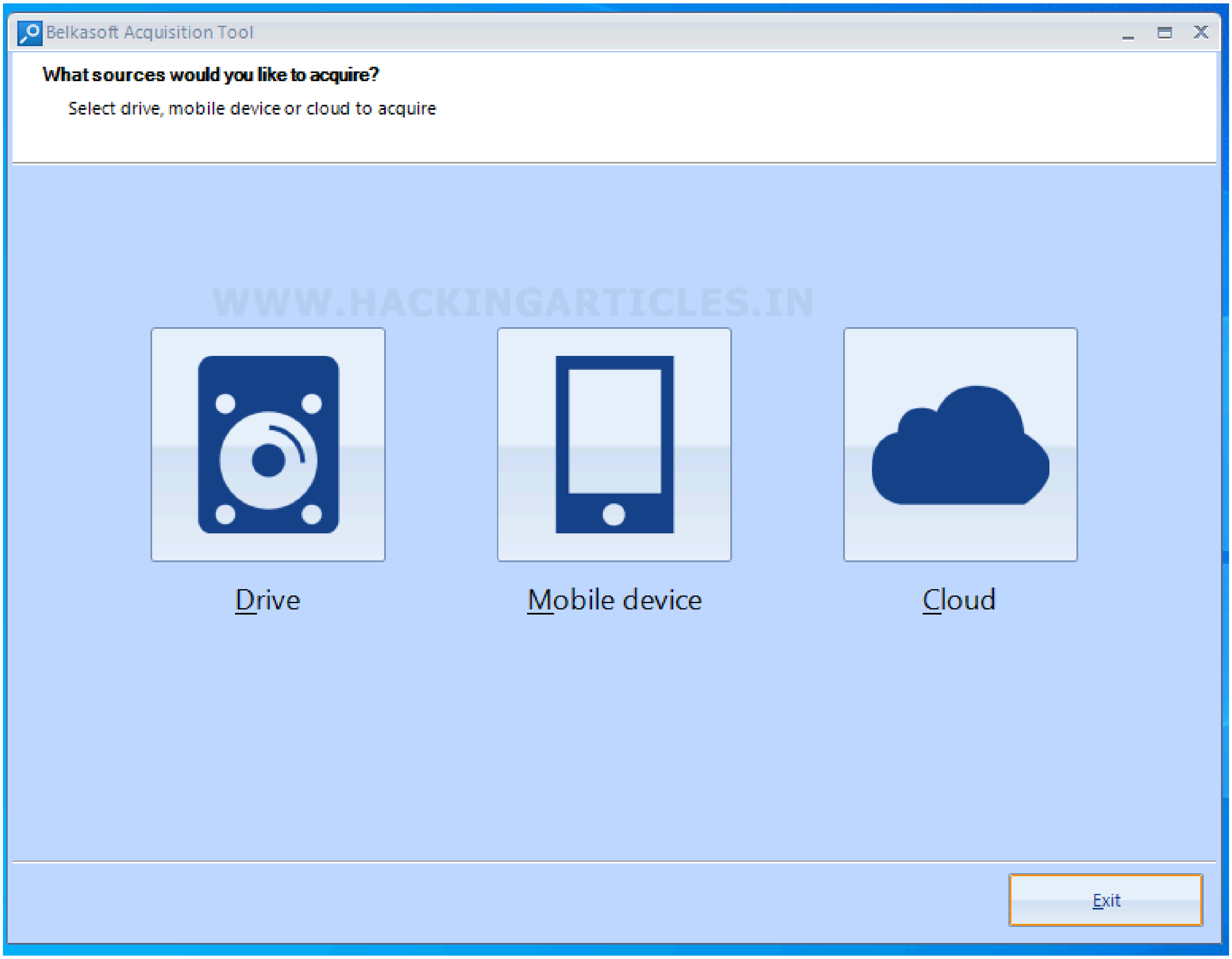
```
C:\Users\Victim\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 0880-91DA

 Directory of C:\Users\Victim\Desktop

25-12-2019  23:22    <DIR>          .
25-12-2019  23:22    <DIR>          ..
25-12-2019  23:15     1,572,864,000 Evidence.raw.001
25-12-2019  23:31             1,747 Evidence.raw.001.txt
25-12-2019  23:16     1,572,864,000 Evidence.raw.002
25-12-2019  23:17     1,572,864,000 Evidence.raw.003
25-12-2019  23:17     1,572,864,000 Evidence.raw.004
25-12-2019  23:18     1,572,864,000 Evidence.raw.005
25-12-2019  23:19     1,572,864,000 Evidence.raw.006
25-12-2019  23:20     1,572,864,000 Evidence.raw.007
25-12-2019  23:21     1,572,864,000 Evidence.raw.008
25-12-2019  23:21     1,572,864,000 Evidence.raw.009
25-12-2019  23:22     1,441,792,000 Evidence.raw.010
25-12-2019  23:24    <DIR>          New Folder
              11 File(s) 15,597,569,747 bytes
               3 Dir(s)  19,586,240,512 bytes free

C:\Users\Victim\Desktop>
```

Belkasoft Acquisition

Belkasoft Acquisitiontool formally known as BAT. This tool can create images of hard drives, Removable drives, Mobile devices, Computer RAM memory, cloud data. The acquired image can be analyzed with any third-party tool.

We can download the belkasoft Acquisitiontool from **here**

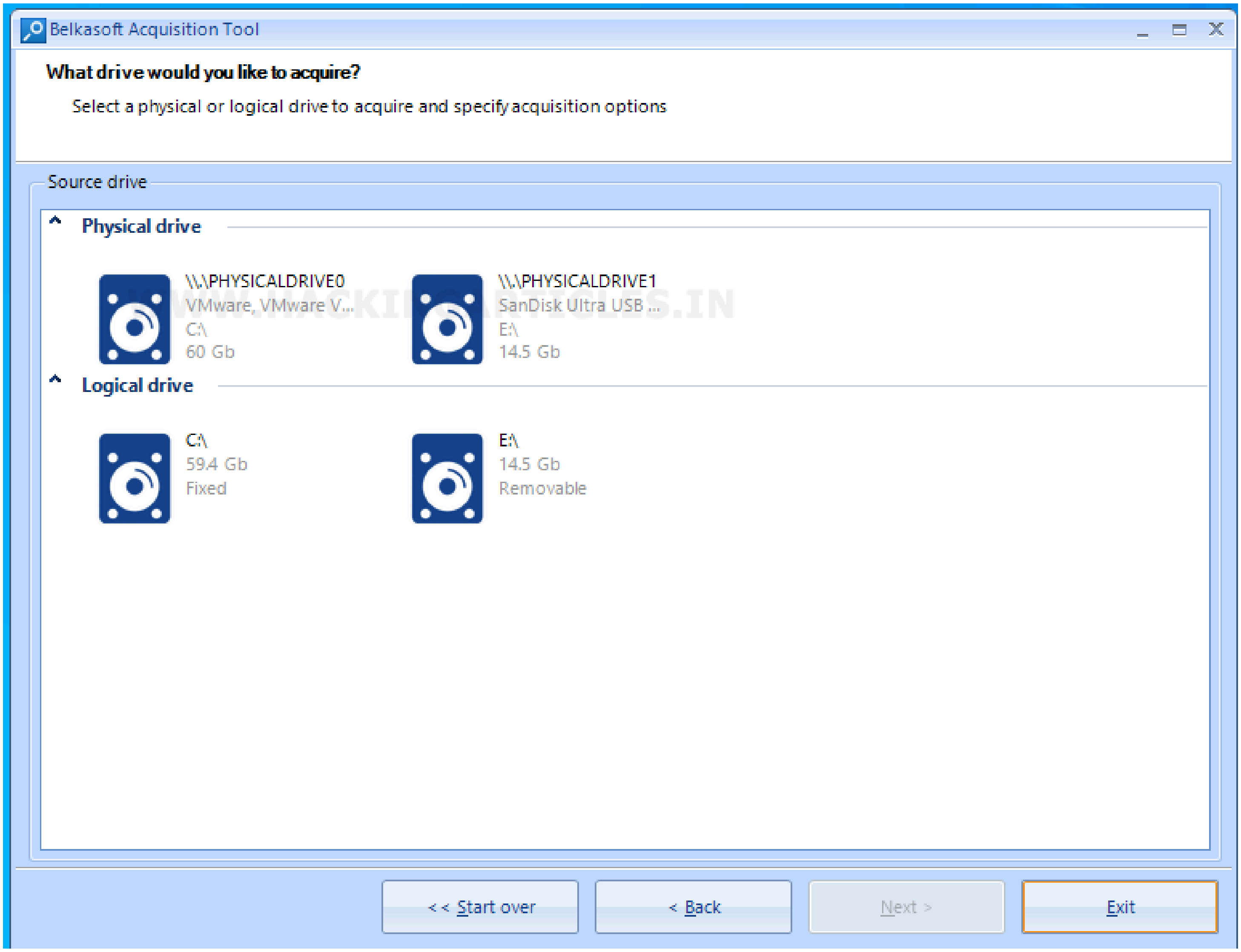
Once the dialogue box opens, click on Drive option.



What sources would you like to acquire?

Select drive, mobile device or cloud to acquire

Now, it will show you all the drives available. From these options select the one drive whose image you want to create and then click on Next button.



What drive would you like to acquire?

Select a physical or logical drive to acquire and specify acquisition options

Source drive

Physical drive

\\.\PHYSICALDRIVE0
VMware, VMware V...
C:\
60 Gb

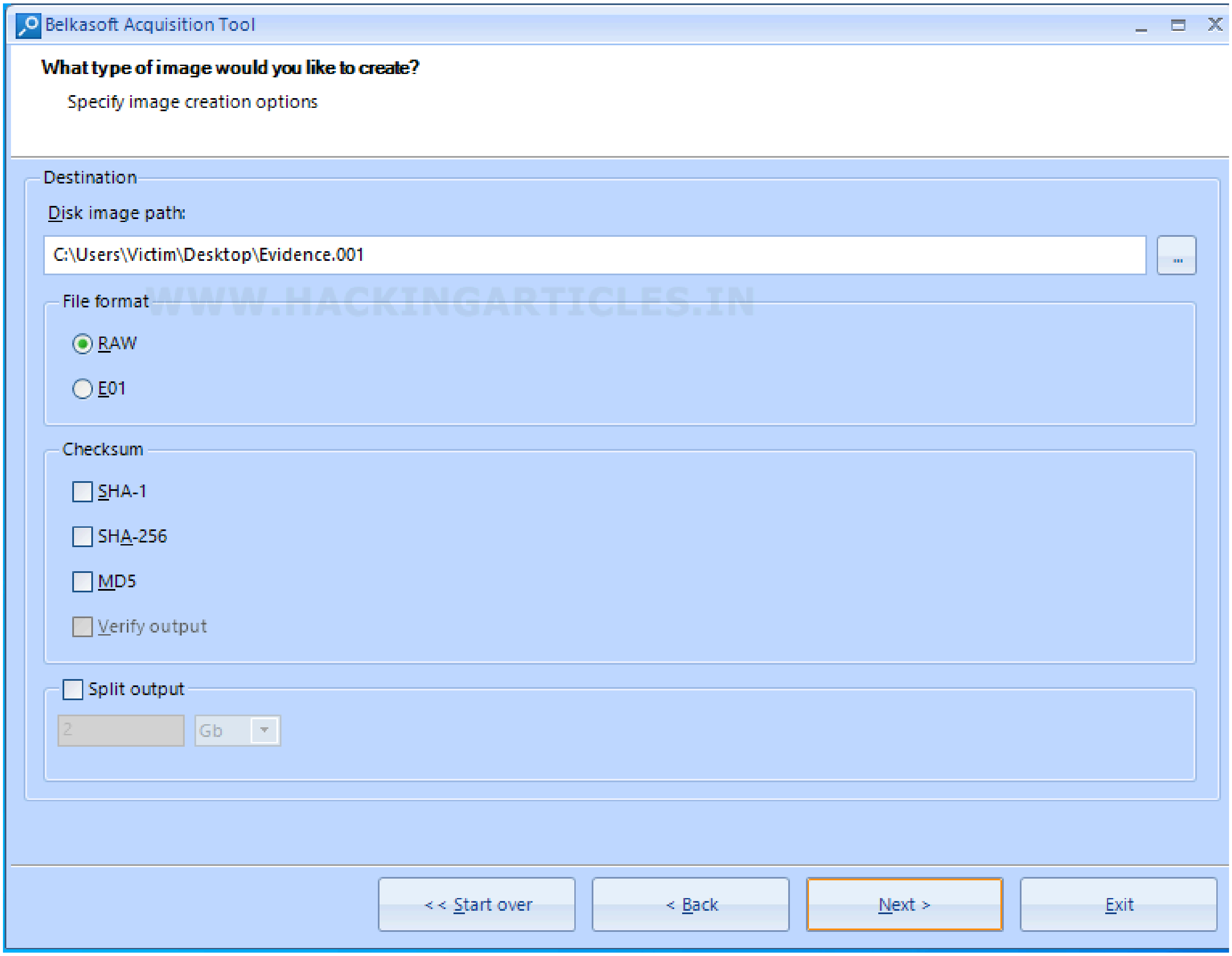
\\.\PHYSICALDRIVE1
SanDisk Ultra USB ...
E:\
14.5 Gb

Logical drive

C:\
59.4 Gb
Fixed

E:\
14.5 Gb
Removable

After selecting the drive, we need to provide the destination path along with the format of image and hash algorithm for the checksum. We can also choose whether to split image or not. And then click on the Next button.



What type of image would you like to create?

Specify image creation options

Destination

Disk image path: C:\Users\Victim\Desktop\Evidence.001

File format

● RAW

○ E01

Checksum

□ SHA-1

□ SHA-256

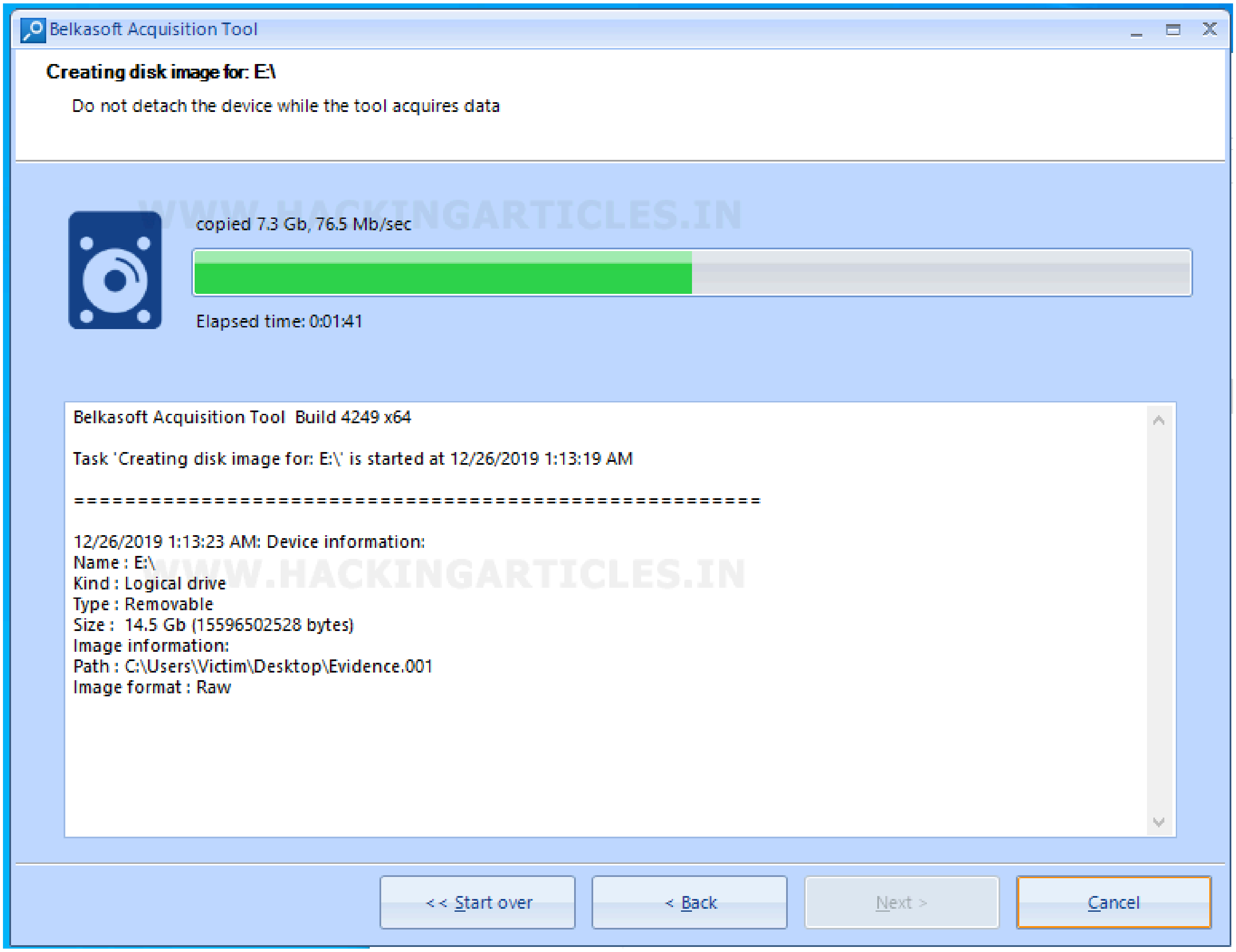
□ MD5

□ Verify output

□ Split output

2 Gb

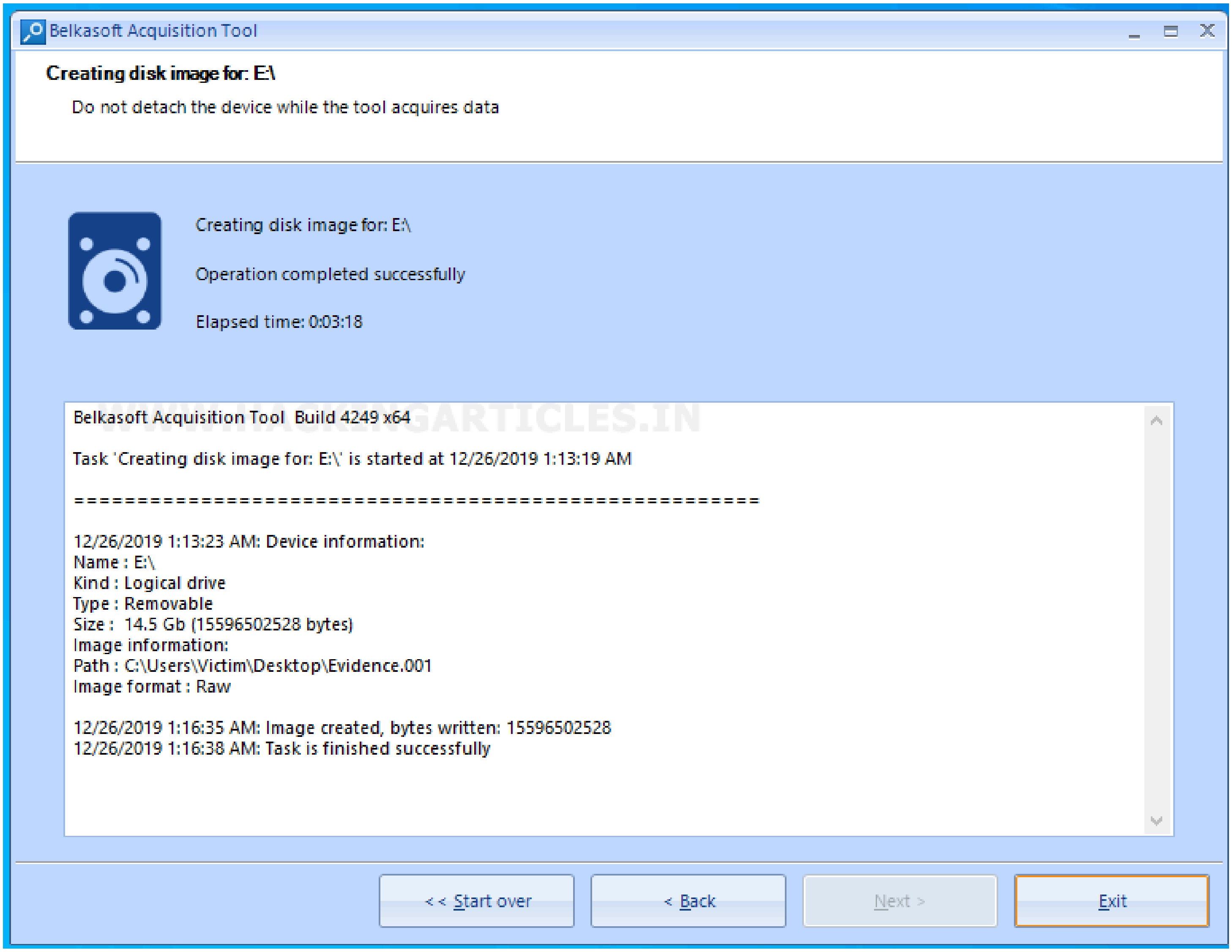
The process of creating the image will start as you can see from the picture below :



Belkasoft Acquisition Tool
Creating disk image for: E:\
Do not detach the device while the tool acquires data
copied 7.3 Gb, 76.5 Mb/sec
Elapsed time: 0:01:41
<< Start over
< Back
Next >
Cancel

```
Belkasoft Acquisition Tool  Build 4249 x64

Task 'Creating disk image for: E:\' is started at 12/26/2019 1:13:19 AM

=======================================================

12/26/2019 1:13:23 AM: Device information:
Name : E:\
Kind : Logical drive
Type : Removable
Size :  14.5 Gb (15596502528 bytes)
Image information:
Path : C:\Users\Victim\Desktop\Evidence.001
Image format : Raw
```

Once the process is complete and the image is created, click on the Exit button.



Creating disk image for: E:\

Do not detach the device while the tool acquires data

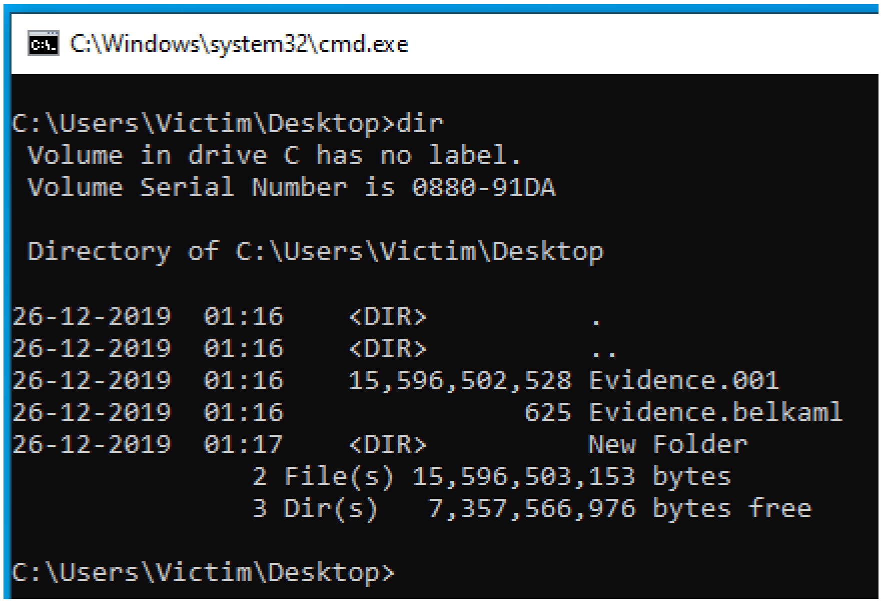
Creating disk image for: E:\

Operation completed successfully

Elapsed time: 0:03:18

```
Belkasoft Acquisition Tool  Build 4249 x64

Task 'Creating disk image for: E:\' is started at 12/26/2019 1:13:19 AM

=========================================================

12/26/2019 1:13:23 AM: Device information:
Name : E:\
Kind : Logical drive
Type : Removable
Size :  14.5 Gb (15596502528 bytes)
Image information:
Path : C:\Users\Victim\Desktop\Evidence.001
Image format : Raw

12/26/2019 1:16:35 AM: Image created, bytes written: 15596502528
12/26/2019 1:16:38 AM: Task is finished successfully
```

To verify the image, go to the destination folder and access it as shown in the picture below :

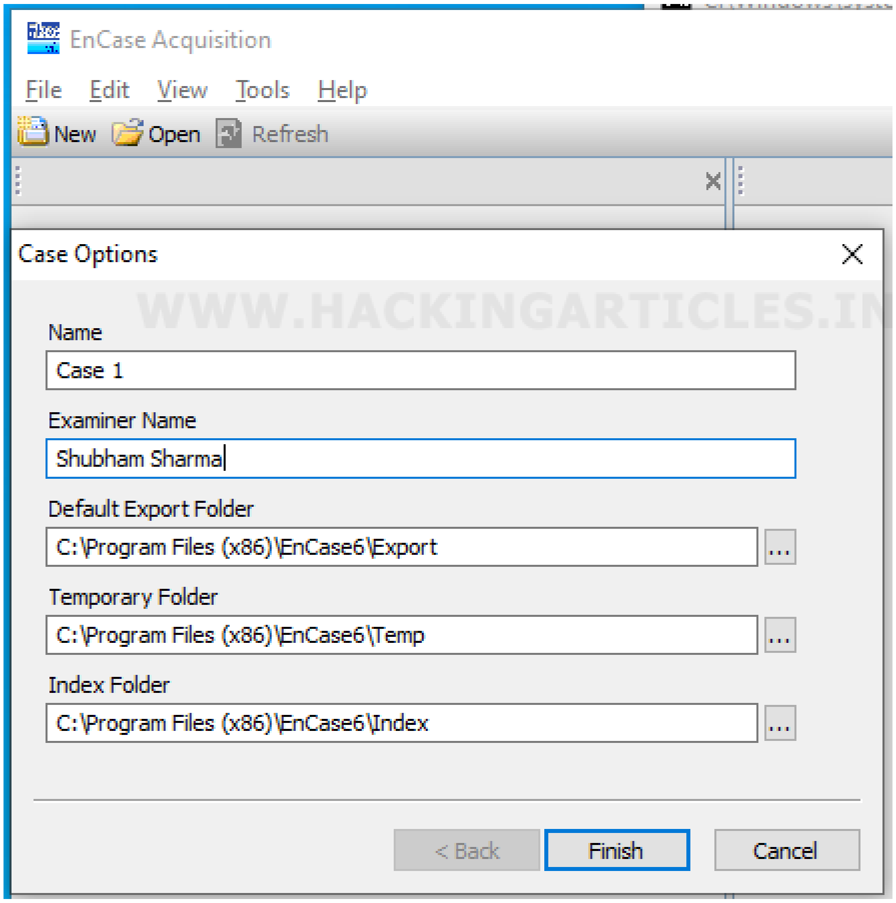


```
C:\Users\Victim\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 0880-91DA

 Directory of C:\Users\Victim\Desktop

26-12-2019  01:16    <DIR>          .
26-12-2019  01:16    <DIR>          ..
26-12-2019  01:16    15,596,502,528 Evidence.001
26-12-2019  01:16               625 Evidence.belkaml
26-12-2019  01:17    <DIR>          New Folder
               2 File(s) 15,596,503,153 bytes
               3 Dir(s)   7,357,566,976 bytes free

C:\Users\Victim\Desktop>
```

Encase Imager

Another way to capture image is by using Encase tool. We can download Encase imager from **here**.

To start the process, firstly, we need to give all the details about the case. And then click on Finish button.



Name: Case 1

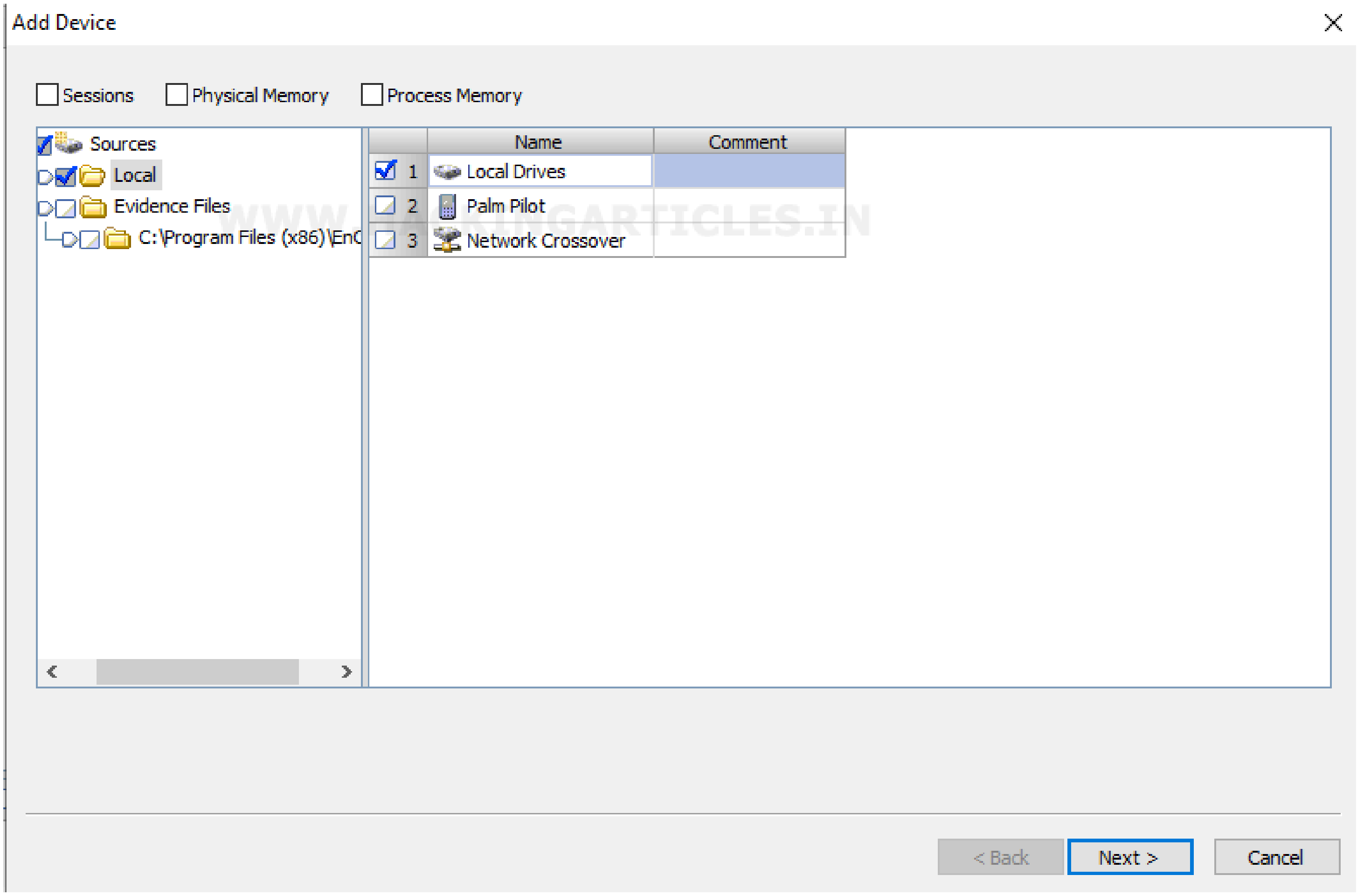
Examiner Name: Shubham Sharma

Default Export Folder: C:\Program Files (x86)\EnCase6\Export

Temporary Folder: C:\Program Files (x86)\EnCase6\Temp

Index Folder: C:\Program Files (x86)\EnCase6\Index

After that, we need to choose the hard drive whose image we want to create. Once you have selected the drive, click on Next button.



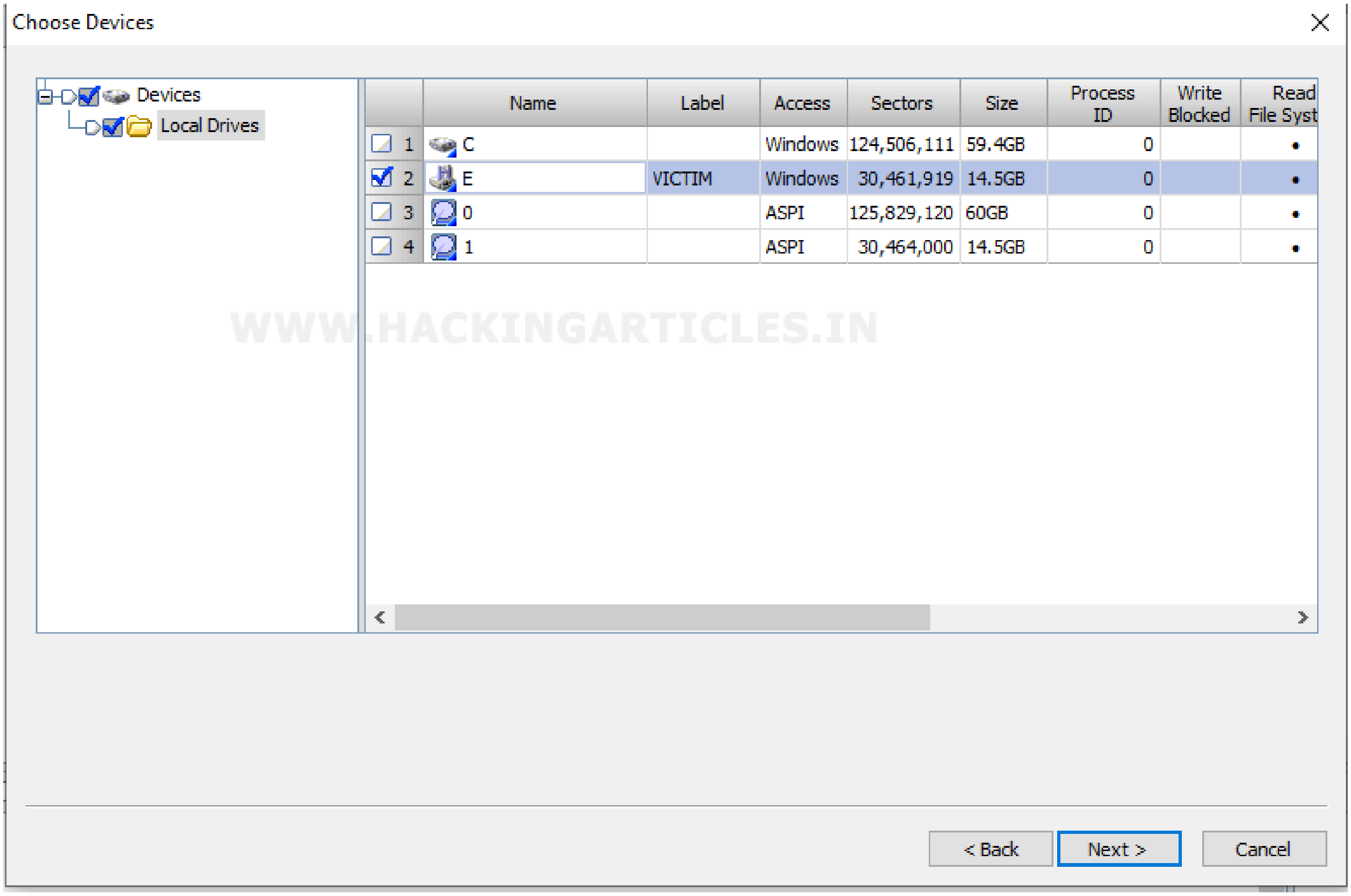
Add Device

□ Sessions □ Physical Memory □ Process Memory

☑ Sources
- ☑ Local
- □ Evidence Files
  - □ C:\Program Files (x86)\EnC

		Name	Comment
☑	1	Local Drives	
□	2	Palm Pilot	
□	3	Network Crossover	

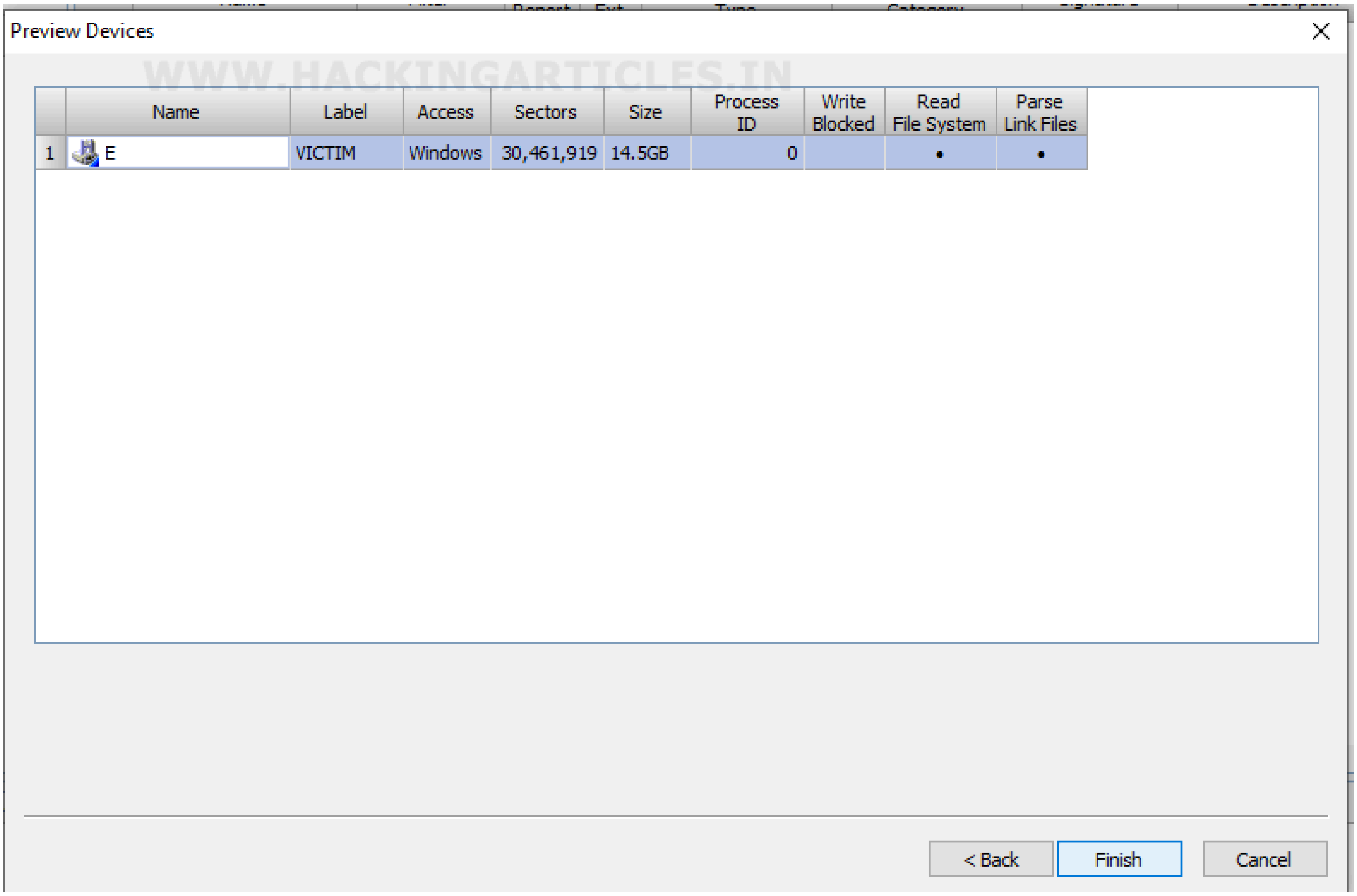
Now, select the specific drive whose image you want to create as shown in the picture below and click on Next button.



- ☑ Devices
  - ☑ Local Drives

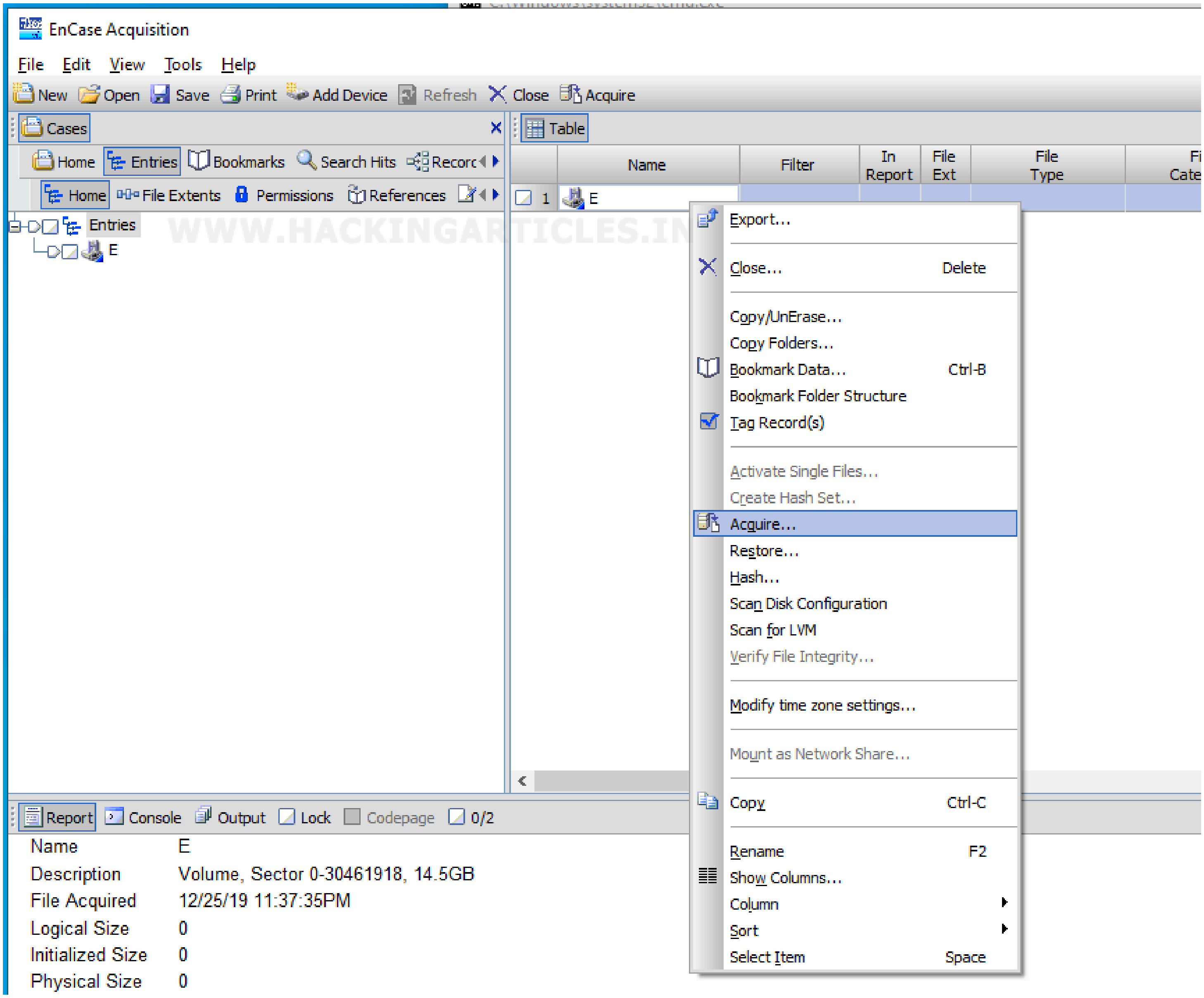
		Name	Label	Access	Sectors	Size	Process ID	Write Blocked	Read File Syst
☐	1	C		Windows	124,506,111	59.4GB	0		•
☑	2	E	VICTIM	Windows	30,461,919	14.5GB	0		•
☐	3	0		ASPI	125,829,120	60GB	0		•
☐	4	1		ASPI	30,464,000	14.5GB	0		•

Then after selecting all the things it asking us to review all the details which were given. Once review is done, click on Finish Button.



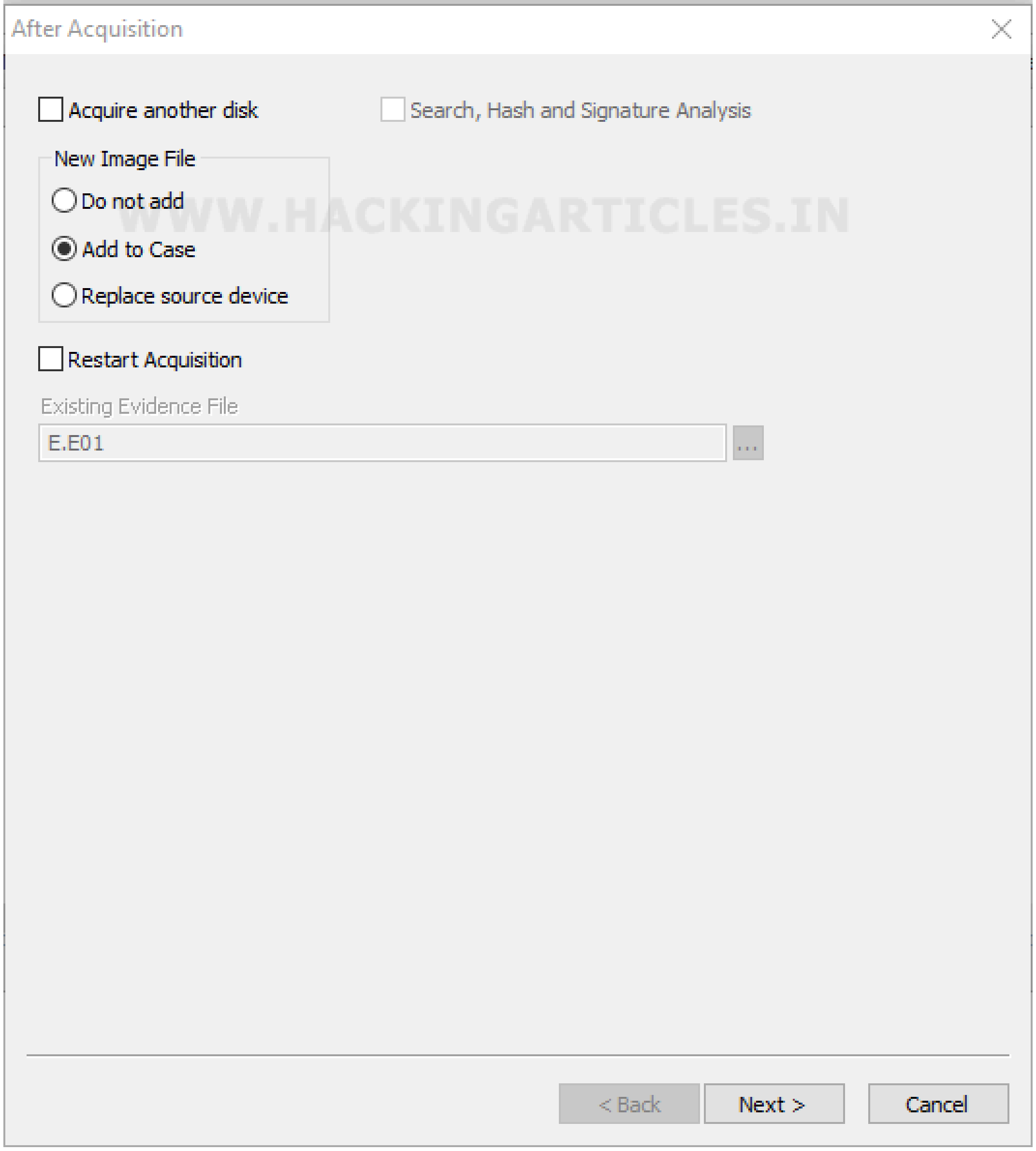
	Name	Label	Access	Sectors	Size	Process ID	Write Blocked	Read File System	Parse Link Files
1	E	VICTIM	Windows	30,461,919	14.5GB	0		•	•

After that, right-click on the chosen driven and then select the Acquire option from the drop-down menu.

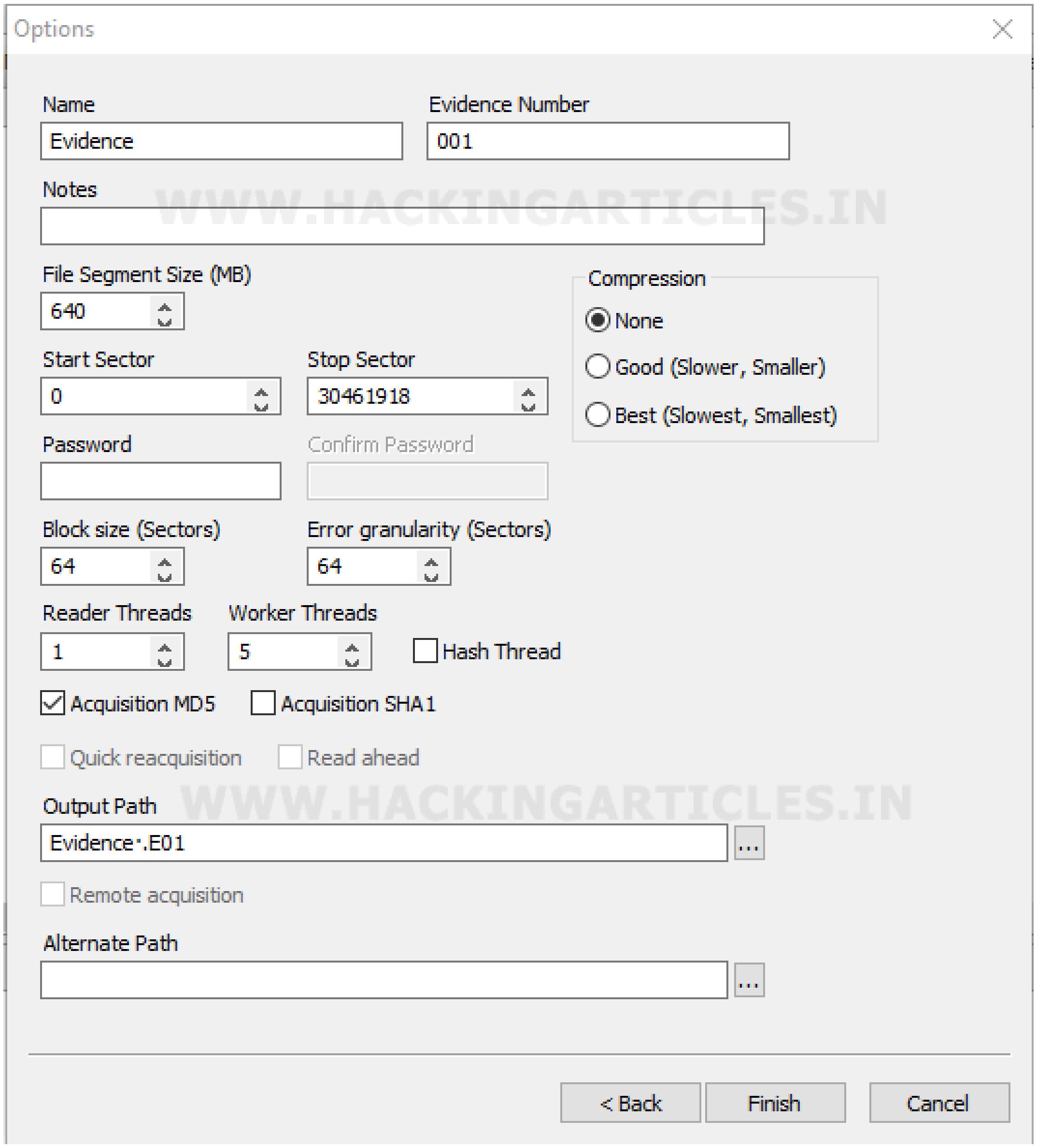

EnCase Acquisition
File Edit View Tools Help
New Open Save Print Add Device Refresh Close Acquire
Cases
Home Entries Bookmarks Search Hits Records
Home File Extents Permissions References
Entries
E
Table
Name Filter In Report File Ext File Type File Category
1 E
Export...
Close... Delete
Copy/UnErase...
Copy Folders...
Bookmark Data... Ctrl-B
Bookmark Folder Structure
Tag Record(s)
Activate Single Files...
Create Hash Set...
Acquire...
Restore...
Hash...
Scan Disk Configuration
Scan for LVM
Verify File Integrity...
Modify time zone settings...
Mount as Network Share...
Copy Ctrl-C
Rename F2
Show Columns...
Column
Sort
Select Item Space
Report Console Output Lock Codepage 0/2

Name	E
Description	Volume, Sector 0-30461918, 14.5GB
File Acquired	12/25/19 11:37:35PM
Logical Size	0
Initialized Size	0
Physical Size	0

After this select the add to case option and then click on Next button.



After this, give the name, number and other details for your image. Then click the finish button.



Options

Name: Evidence

Evidence Number: 001

Notes:

File Segment Size (MB): 640

Start Sector: 0

Stop Sector: 30461918

Password:

Confirm Password:

Block size (Sectors): 64

Error granularity (Sectors): 64

Reader Threads: 1

Worker Threads: 5

□ Hash Thread

☑ Acquisition MD5

□ Acquisition SHA1

□ Quick reacquisition

□ Read ahead

Output Path: Evidence·.E01

□ Remote acquisition

Alternate Path:

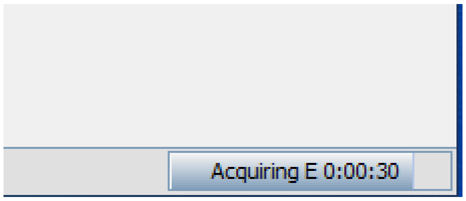
Compression

● None

○ Good (Slower, Smaller)

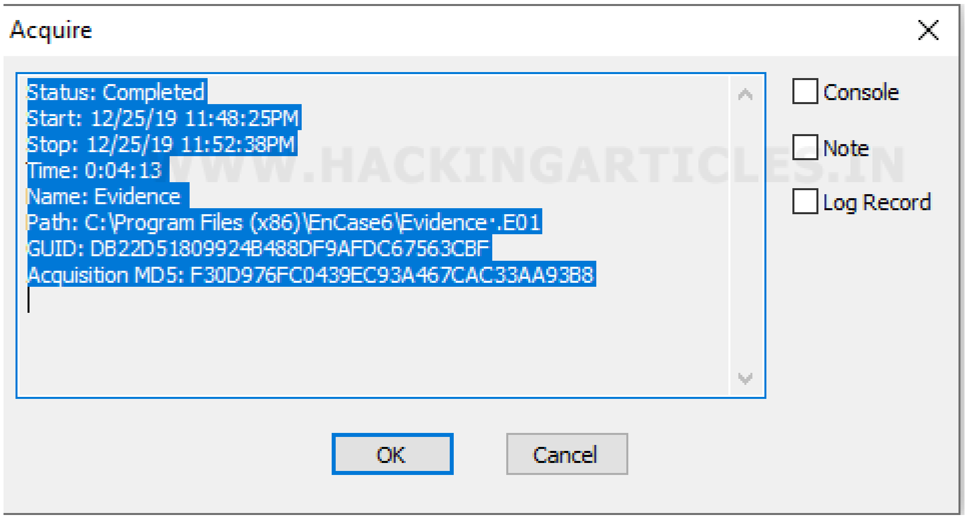
○ Best (Slowest, Smallest)

After clicking on the finish button, you can observe that on the right-hand side, the lower section of the encase window will show the status of the process.



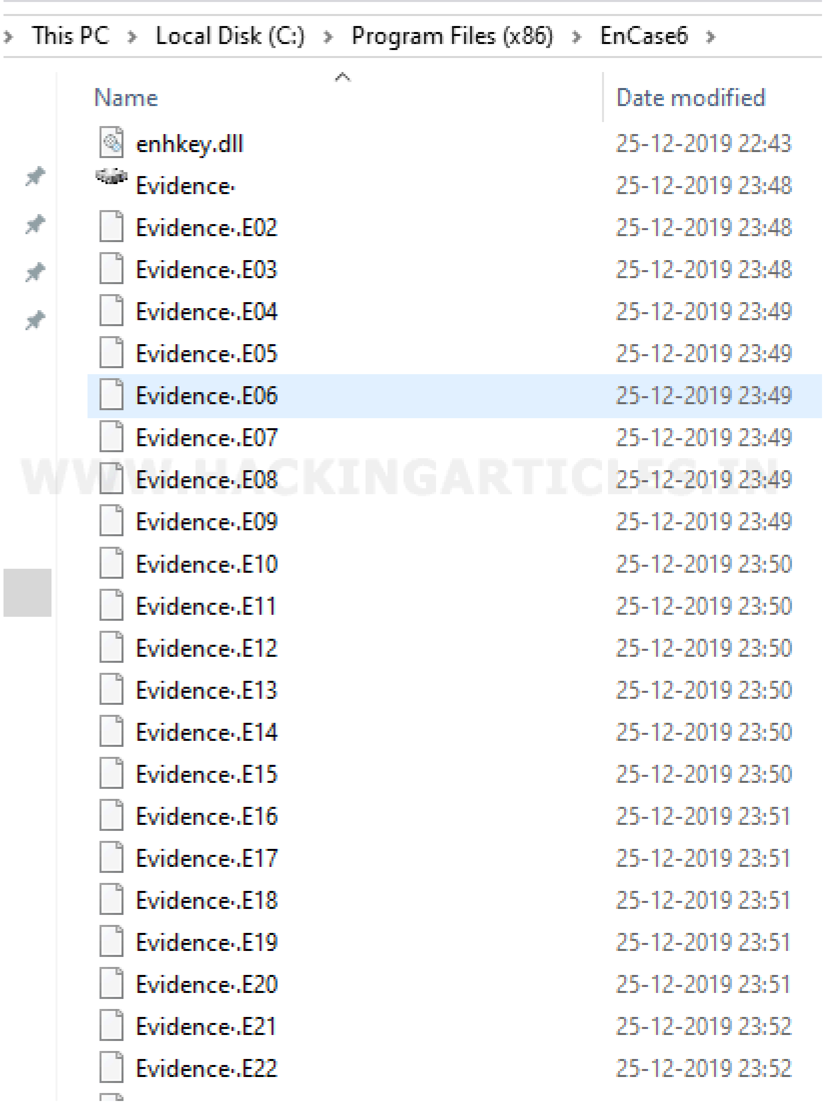
Acquiring E 0:00:30

After everything is done, it will show you all the details like status, start time, name, process id, destination path, the total time for the whole acquiring image, images hashes. And then at last, you can click on OK.



```
Status: Completed
Start: 12/25/19 11:48:25PM
Stop: 12/25/19 11:52:38PM
Time: 0:04:13
Name: Evidence
Path: C:\Program Files (x86)\EnCase6\Evidence·.E01
GUID: DB22D51809924B488DF9AFDC67563CBF
Acquisition MD5: F30D976FC0439EC93A467CAC33AA93B8
```

Once the image is created, you can see that Encase uses E01 format while creating an image and further splits it into multiple parts as shown in the picture below:



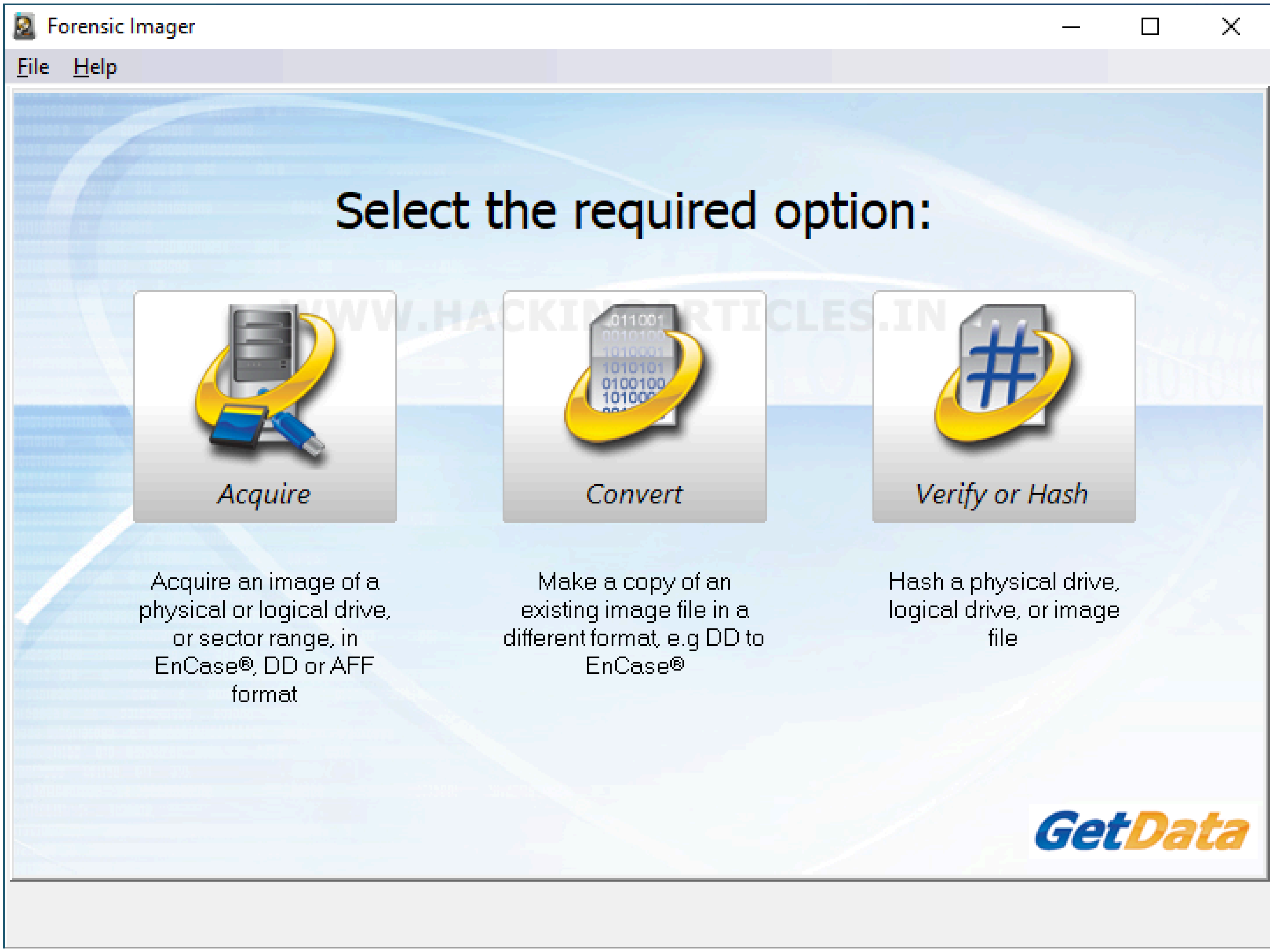
› This PC › Local Disk (C:) › Program Files (x86) › EnCase6 ›

Name	Date modified
enhkey.dll	25-12-2019 22:43
Evidence·	25-12-2019 23:48
Evidence·.E02	25-12-2019 23:48
Evidence·.E03	25-12-2019 23:48
Evidence·.E04	25-12-2019 23:49
Evidence·.E05	25-12-2019 23:49
Evidence·.E06	25-12-2019 23:49
Evidence·.E07	25-12-2019 23:49
Evidence·.E08	25-12-2019 23:49
Evidence·.E09	25-12-2019 23:49
Evidence·.E10	25-12-2019 23:50
Evidence·.E11	25-12-2019 23:50
Evidence·.E12	25-12-2019 23:50
Evidence·.E13	25-12-2019 23:50
Evidence·.E14	25-12-2019 23:50
Evidence·.E15	25-12-2019 23:50
Evidence·.E16	25-12-2019 23:51
Evidence·.E17	25-12-2019 23:51
Evidence·.E18	25-12-2019 23:51
Evidence·.E19	25-12-2019 23:51
Evidence·.E20	25-12-2019 23:51
Evidence·.E21	25-12-2019 23:52
Evidence·.E22	25-12-2019 23:52

Forensics Imager

Another way to capture an image is by using forensic imager. We can download Forensic imager from **here**.

To start the process, click on Acquire button as shown in the image.

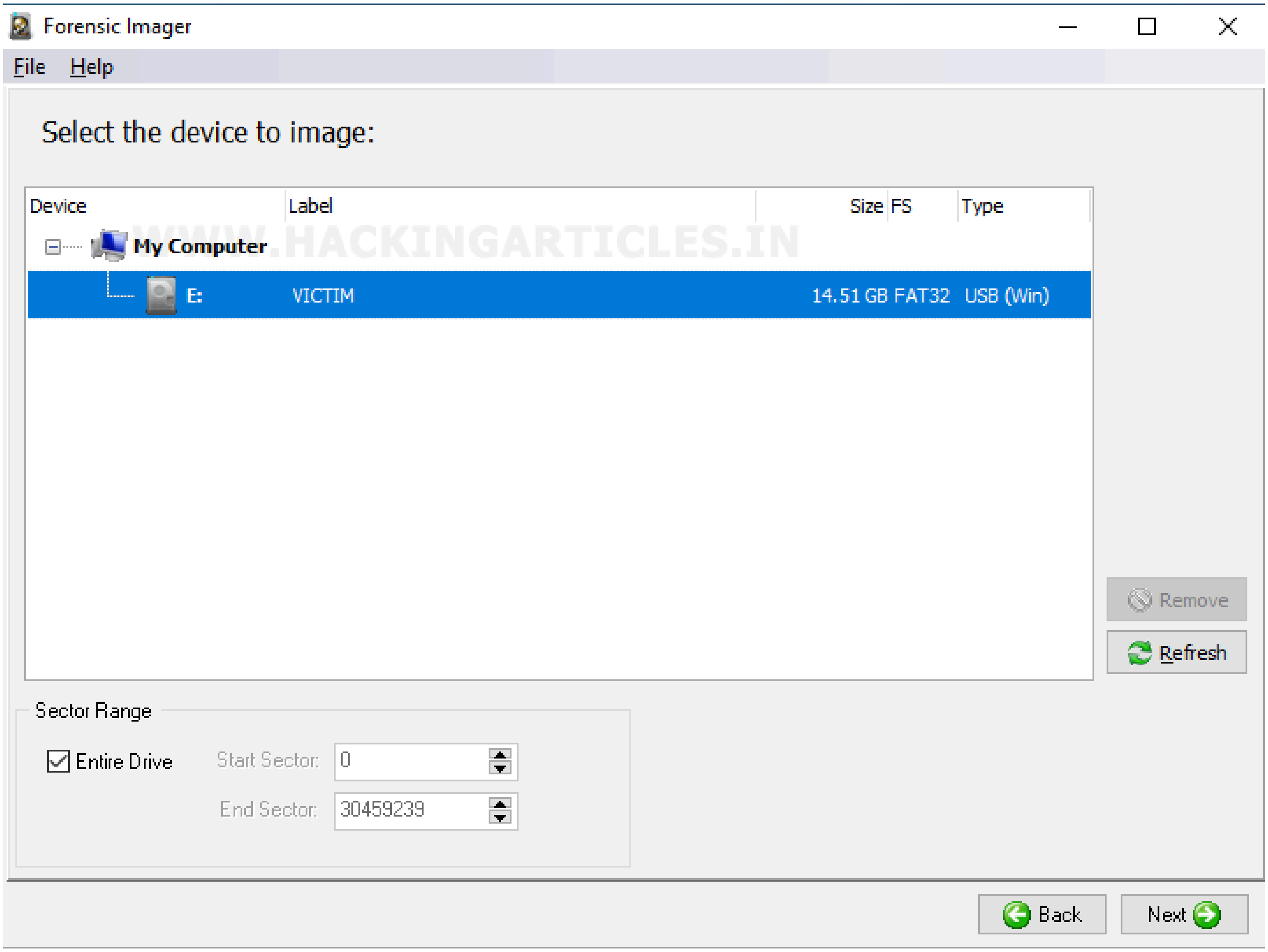


Acquire an image of a physical or logical drive, or sector range, in EnCase®, DD or AFF format

Make a copy of an existing image file in a different format, e.g DD to EnCase®

Hash a physical drive, logical drive, or image file

Next, it will ask you the source to acquire image.



Select the device to image:

Device	Label	Size	FS	Type
My Computer				
E:	VICTIM	14.51 GB	FAT32	USB (Win)

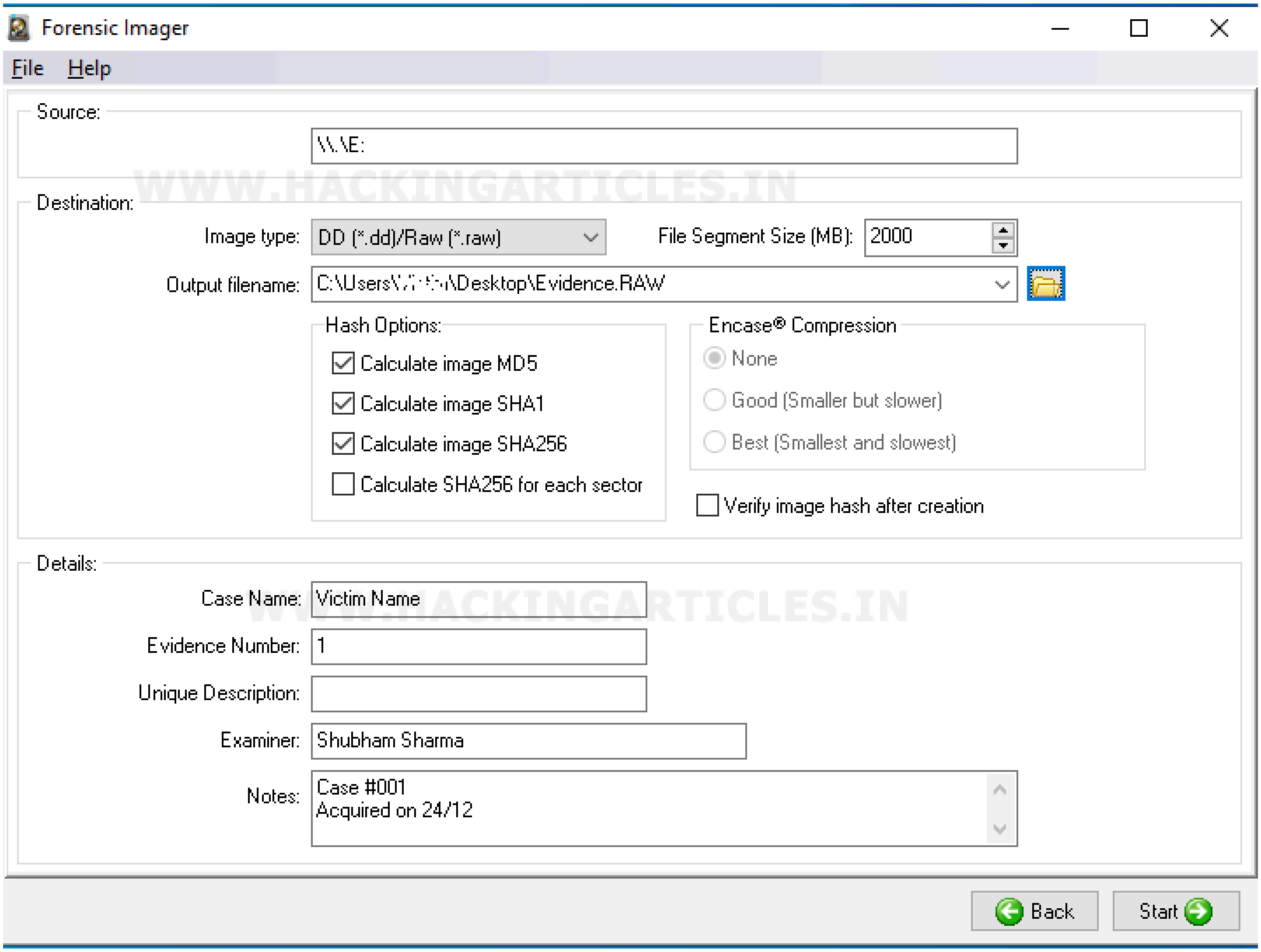
Sector Range

☑ Entire Drive

Start Sector: 0

End Sector: 30459239

As you have given the source for the image, then it will ask you the destination details i.e. the path, format, checksum and other evidence related details. Once you fill all these up, click on Start button.



Source: \\.\E:

Destination:

Image type: DD (*.dd)/Raw (*.raw)

File Segment Size (MB): 2000

Output filename: C:\Users\[illegible]\Desktop\Evidence.RAW

Hash Options:

- ☑ Calculate image MD5
- ☑ Calculate image SHA1
- ☑ Calculate image SHA256
- □ Calculate SHA256 for each sector

Encase® Compression

- ● None
- ○ Good (Smaller but slower)
- ○ Best (Smallest and slowest)

□ Verify image hash after creation

Details:

Case Name: Victim Name

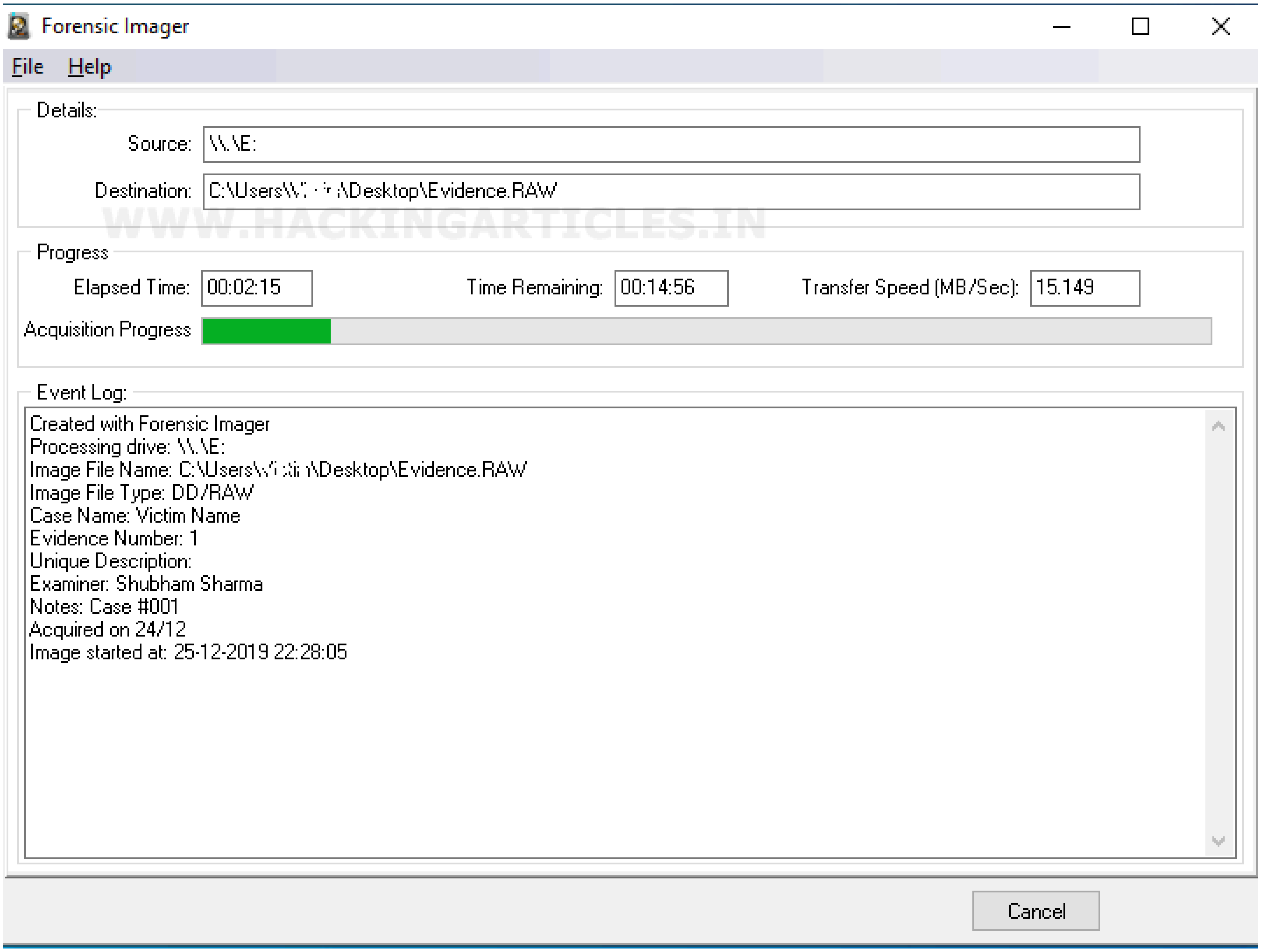
Evidence Number: 1

Unique Description:

Examiner: Shubham Sharma

Notes: Case #001
Acquired on 24/12

After clicking on start, you can observe that the process has begun as shown in the picture below :



Details:

Source: \\.\E:

Destination: C:\Users\[redacted]\Desktop\Evidence.RAW

Progress

Elapsed Time: 00:02:15

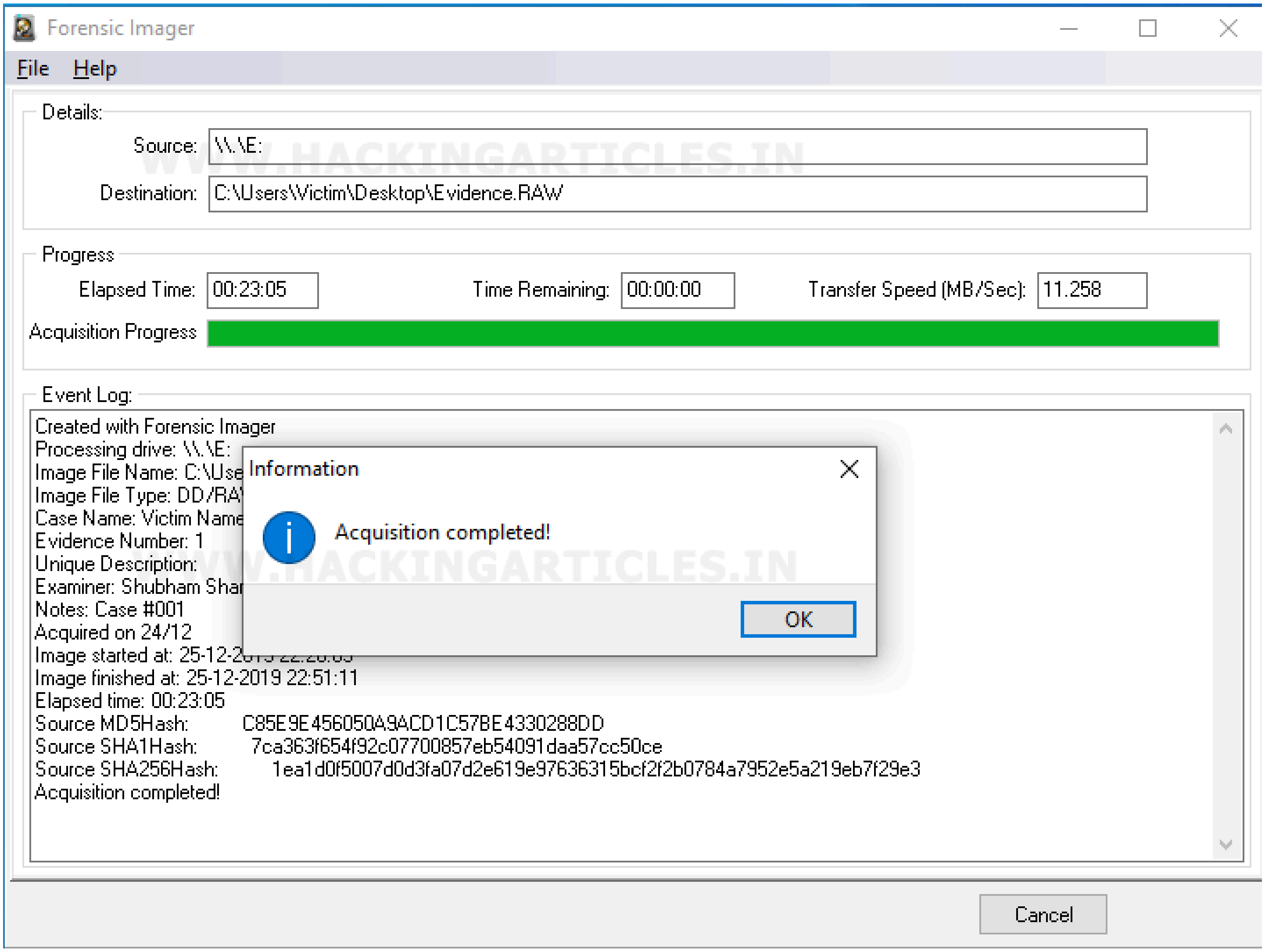
Time Remaining: 00:14:56

Transfer Speed (MB/Sec): 15.149

Event Log:

```
Created with Forensic Imager
Processing drive: \\.\E:
Image File Name: C:\Users\[redacted]\Desktop\Evidence.RAW
Image File Type: DD/RAW
Case Name: Victim Name
Evidence Number: 1
Unique Description:
Examiner: Shubham Sharma
Notes: Case #001
Acquired on 24/12
Image started at: 25-12-2019 22:28:05
```

After completing the process, it will show you a pop-up message saying acquisition completed. It means that our forensic image is created. In order to check we need to check the destination path to verify our forensic image.



Details:

Source: \\.\E:

Destination: C:\Users\Victim\Desktop\Evidence.RAW

Progress

Elapsed Time: 00:23:05

Time Remaining: 00:00:00

Transfer Speed (MB/Sec): 11.258

Acquisition Progress

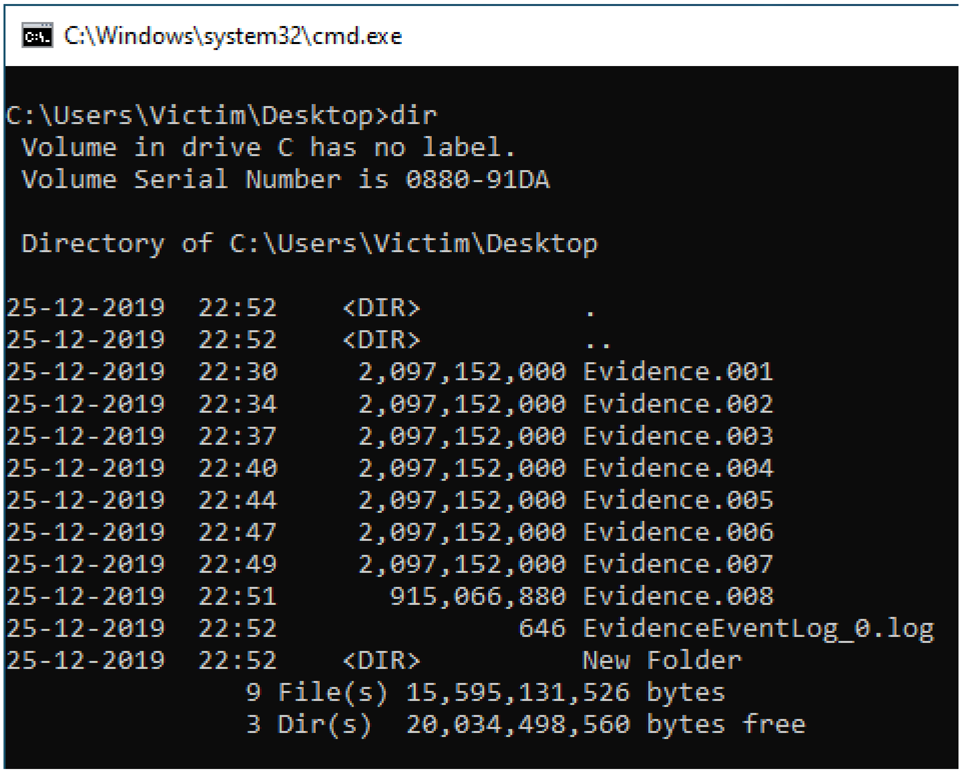
Event Log:

```
Created with Forensic Imager
Processing drive: \\.\E:
Image File Name: C:\Use
Image File Type: DD/RA
Case Name: Victim Name
Evidence Number: 1
Unique Description:
Examiner: Shubham Shar
Notes: Case #001
Acquired on 24/12
Image started at: 25-12-2
Image finished at: 25-12-2019 22:51:11
Elapsed time: 00:23:05
Source MD5Hash:        C85E9E456050A9ACD1C57BE4330288DD
Source SHA1Hash:        7ca363f654f92c07700857eb54091daa57cc50ce
Source SHA256Hash:        1ea1d0f5007d0d3fa07d2e619e97636315bcf2f2b0784a7952e5a219eb7f29e3
Acquisition completed!
```

Information

Acquisition completed!

We checked at the destination our image is successfully created and ready to be analyzed as a piece of evidence for the forensic investigation.



```
C:\Users\Victim\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 0880-91DA

 Directory of C:\Users\Victim\Desktop

25-12-2019  22:52    <DIR>          .
25-12-2019  22:52    <DIR>          ..
25-12-2019  22:30     2,097,152,000 Evidence.001
25-12-2019  22:34     2,097,152,000 Evidence.002
25-12-2019  22:37     2,097,152,000 Evidence.003
25-12-2019  22:40     2,097,152,000 Evidence.004
25-12-2019  22:44     2,097,152,000 Evidence.005
25-12-2019  22:47     2,097,152,000 Evidence.006
25-12-2019  22:49     2,097,152,000 Evidence.007
25-12-2019  22:51       915,066,880 Evidence.008
25-12-2019  22:52               646 EvidenceEventLog_0.log
25-12-2019  22:52    <DIR>          New Folder
               9 File(s) 15,595,131,526 bytes
               3 Dir(s)  20,034,498,560 bytes free
```

So, these were the five ways to capture a forensic image of a Hard drive. One should always the various ways to create an image as various times calls for various measures.