Ex-7-File Types

Forensics investigators often encounter file types that are not known to them. They have to be careful since even though a file has a particular extension it does not mean that is the true format of the file.

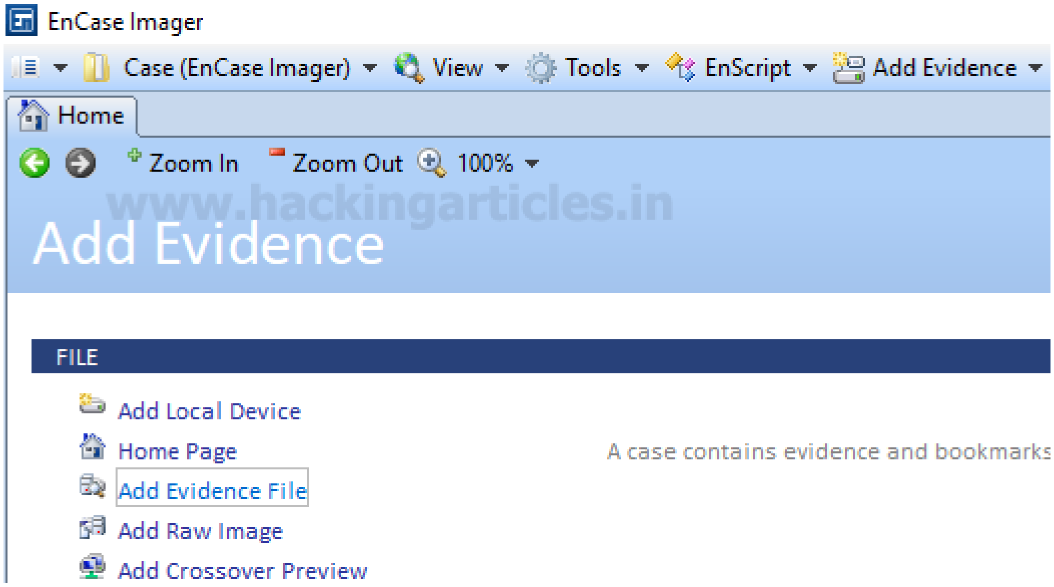
For the following file extensions identify the type of files. Do a Web search if needed.

Jpg jpeg png gif tif tiff bmp art pcx wmf emf dwg psd rtf xml html htm php3 php4 phtml shtml eml dbx pst xls doc docx dot ppt pps pdf zip rar gz bz2 arj wav avi ram rm mpg mpeg mov asf mid

Ex-8

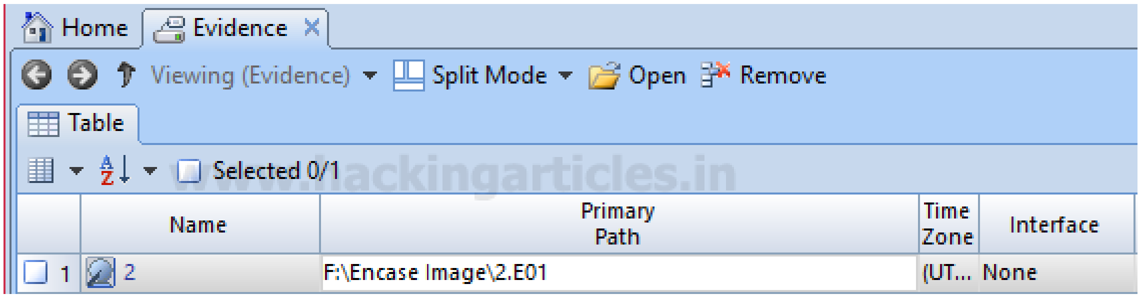
How to Restoring the Evidence Image using EnCase Imager

Open Encase Imager and add the evidence to Encase imager



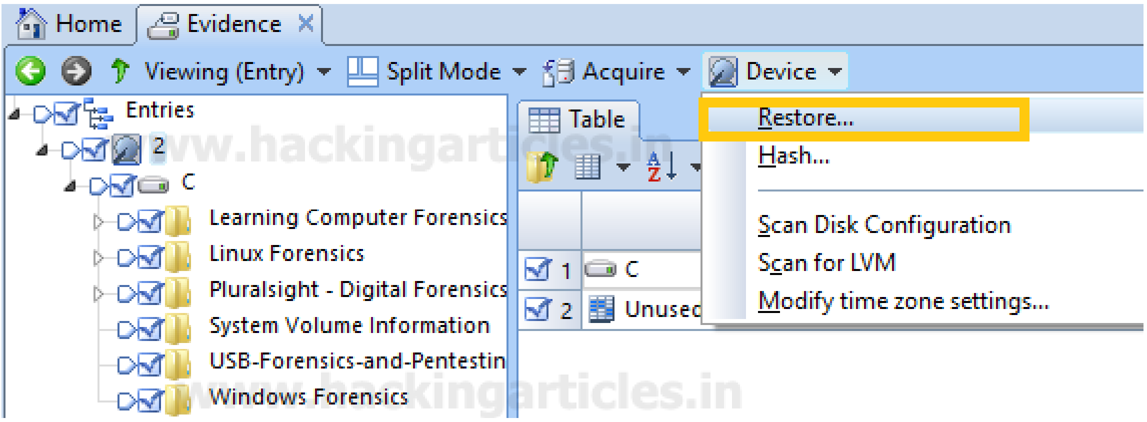
A case contains evidence and bookmarks

Browse to the image (.E01) file and add it to the case. The evidence added will get listed

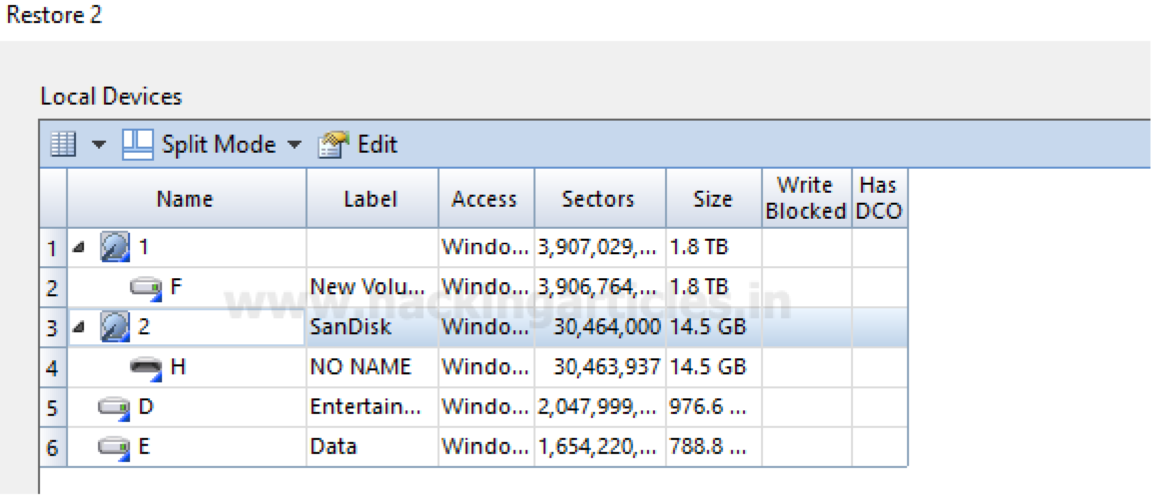


	Name	Primary Path	Time Zone	Interface
□ 1	2	F:\Encase Image\2.E01	(UT...	None

Double click on the image, select he files to be restored and select the restore option located under Device option.

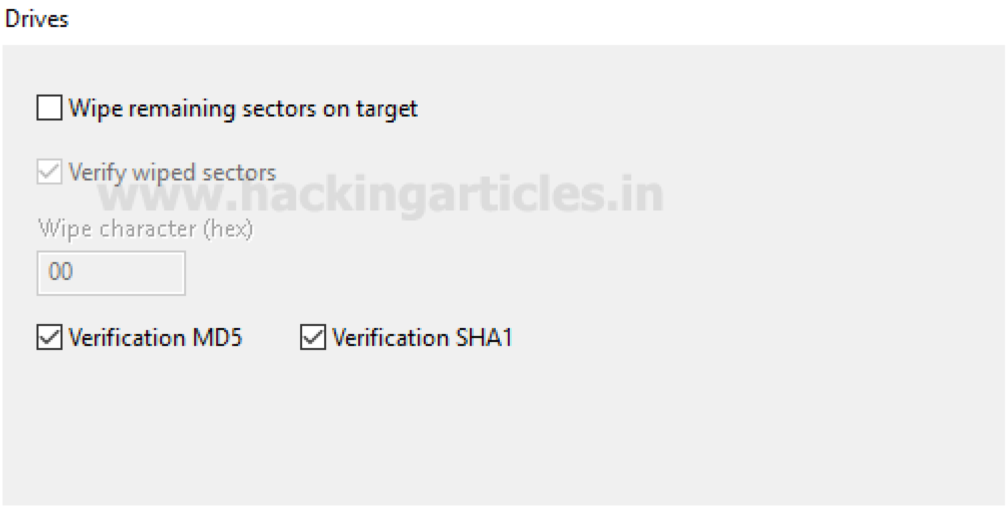


When we click on restore, connect the drive where we want to restore the image and click next. All the drives will be read. All the drives will be displayed, select the drive where the image is to be restored. Use the blank drive for restoring the image as the existing data will be wiped.



	Name	Label	Access	Sectors	Size	Write Blocked	Has DCO
1	1		Windo...	3,907,029,...	1.8 TB		
2	F	New Volu...	Windo...	3,906,764,...	1.8 TB		
3	2	SanDisk	Windo...	30,464,000	14.5 GB		
4	H	NO NAME	Windo...	30,463,937	14.5 GB		
5	D	Entertain...	Windo...	2,047,999,...	976.6 ...		
6	E	Data	Windo...	1,654,220,...	788.8 ...		

If required we can verify the Hash values and click on finish.



Drives

☐ Wipe remaining sectors on target

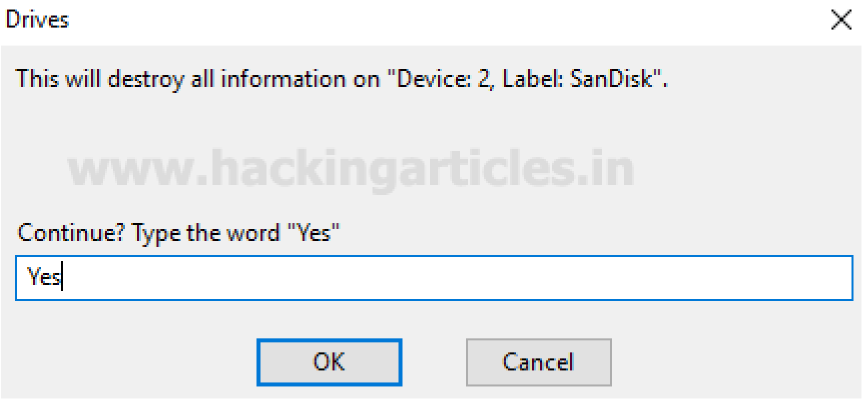
☑ Verify wiped sectors

Wipe character (hex)

00

☑ Verification MD5 ☑ Verification SHA1

Type “Yes” in the text box and click on OK this will wipe the existing data on the drive and start with the image restoration.



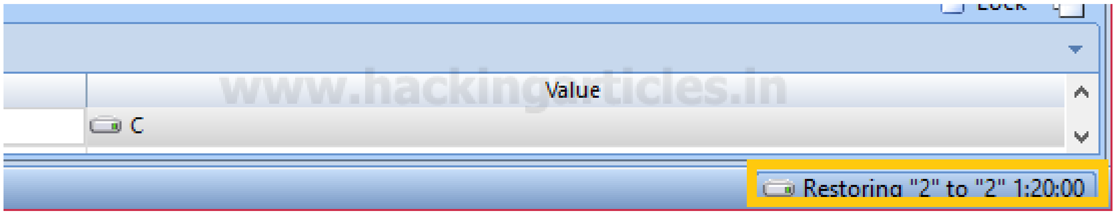
Drives

This will destroy all information on "Device: 2, Label: SanDisk".

Continue? Type the word "Yes"

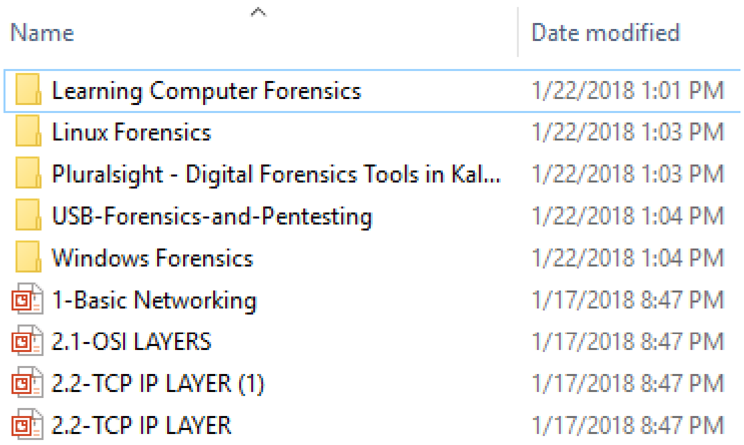
Yes

Image Restoration will start, we can check the progress on the lower right corner of the window.



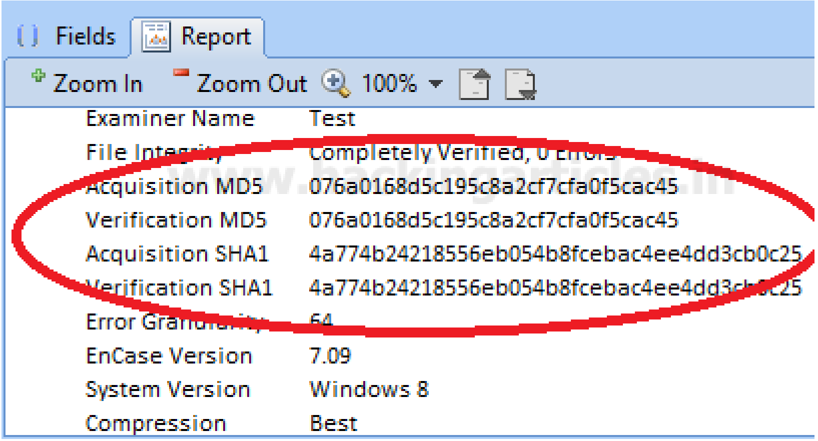
Restoring "2" to "2" 1:20:00

Once the restoration is complete, we can see the data in the drive we have selected.



Name	Date modified
Learning Computer Forensics	1/22/2018 1:01 PM
Linux Forensics	1/22/2018 1:03 PM
Pluralsight - Digital Forensics Tools in Kal...	1/22/2018 1:03 PM
USB-Forensics-and-Pentesting	1/22/2018 1:04 PM
Windows Forensics	1/22/2018 1:04 PM
1-Basic Networking	1/17/2018 8:47 PM
2.1-OSI LAYERS	1/17/2018 8:47 PM
2.2-TCP IP LAYER (1)	1/17/2018 8:47 PM
2.2-TCP IP LAYER	1/17/2018 8:47 PM

To ensure the integrity of the data, we can see the report section on the bottom pane and check the hash values. The hash values should be the same as of the image (we can check the original hash value in the image report.)



Examiner Name	Test
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	076a0168d5c195c8a2cf7cfa0f5cac45
Verification MD5	076a0168d5c195c8a2cf7cfa0f5cac45
Acquisition SHA1	4a774b24218556eb054b8fcebac4ee4dd3cb0c25
Verification SHA1	4a774b24218556eb054b8fcebac4ee4dd3cb0c25
Error Granularity	64
EnCase Version	7.09
System Version	Windows 8
Compression	Best

If required we can copy and save the report in any text / word file for any future reference.