Digital Forensics Investigation using OS Forensics (Part1)

January 29, 2018 By Raj Chandel

About Forensics

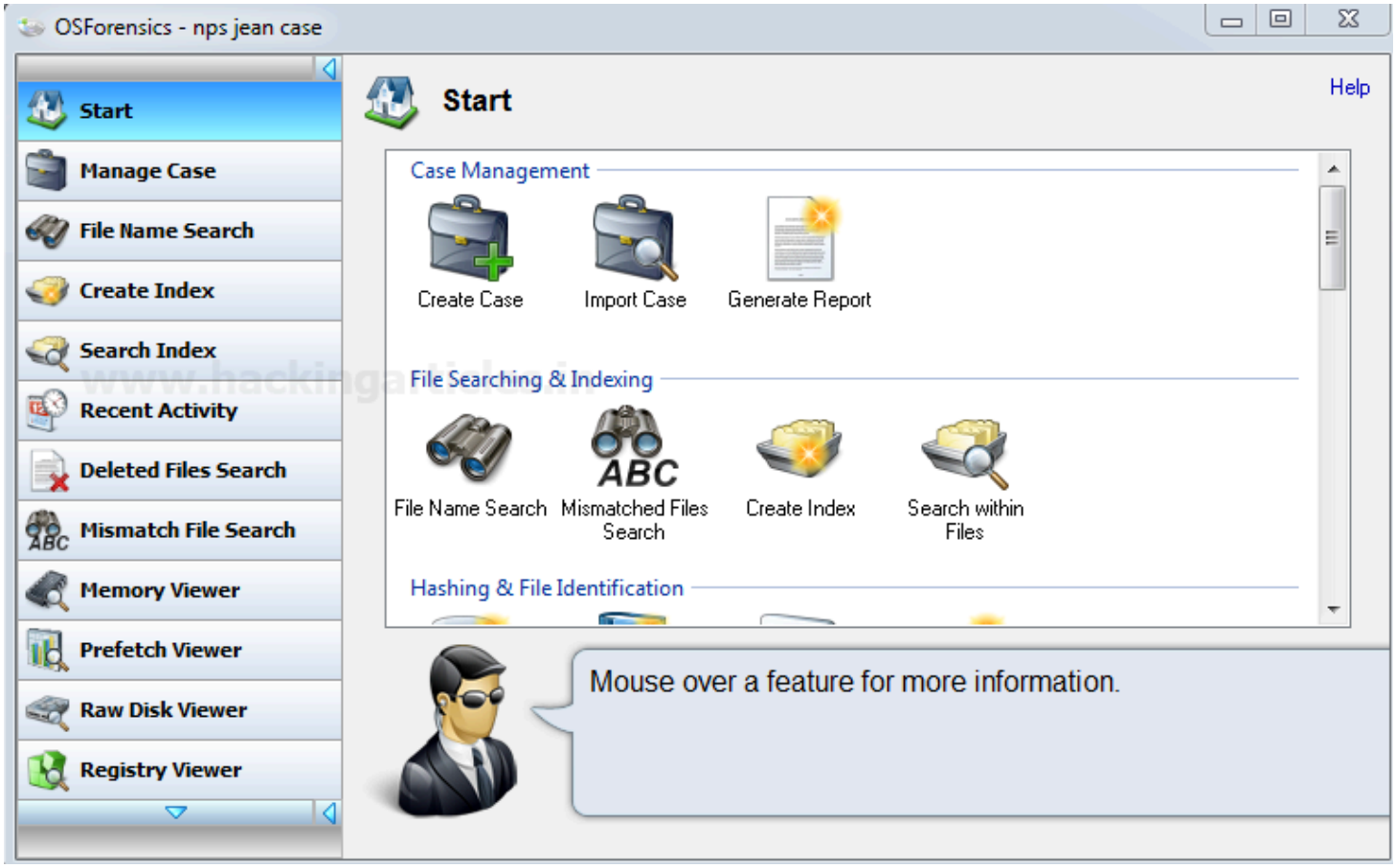
OSForensics from PassMark Software is a digital computer forensic application which lets you extract and analyze digital data evidence efficiently and with ease. It discovers, identifies and manages ie uncovers everything hidden inside your computer systems and digital storage devices.

OSForensics is a self-capable and standalone toolkit which has almost all the digital forensics capabilities including Data acquisition, extraction, analysis, email analysis, data imaging, image restoration and much more.

In this article, we will cover all the major capabilities of OSForensics for digital forensics investigations.

Undiscovering OSForensics

To start with open OSForensics, we can see the OSForensics window open.



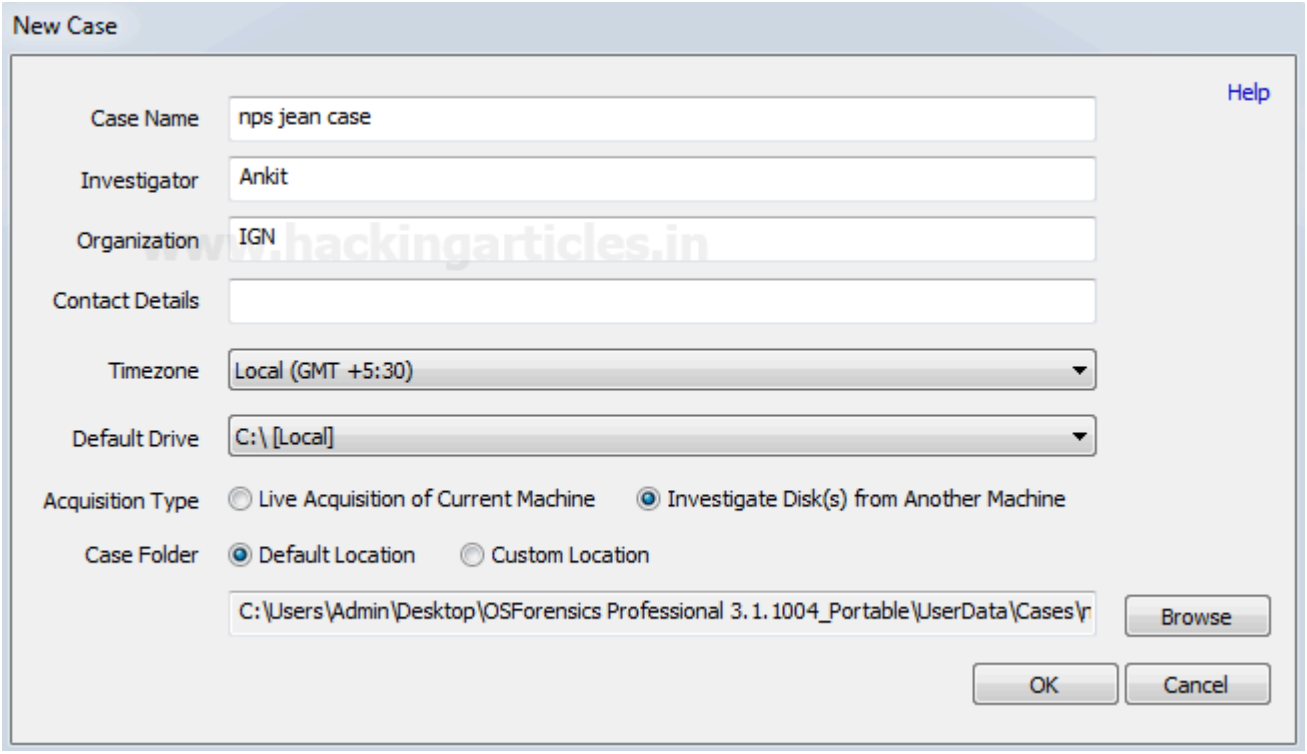
On the left-hand side are the main options/ capabilities of forensic we will be talking about in details.

Please note that the start option highlights the main tools. Features of OSF which are widely used the same options can also be accessed through the tabs on the left pane.

The first option is Manage Case:

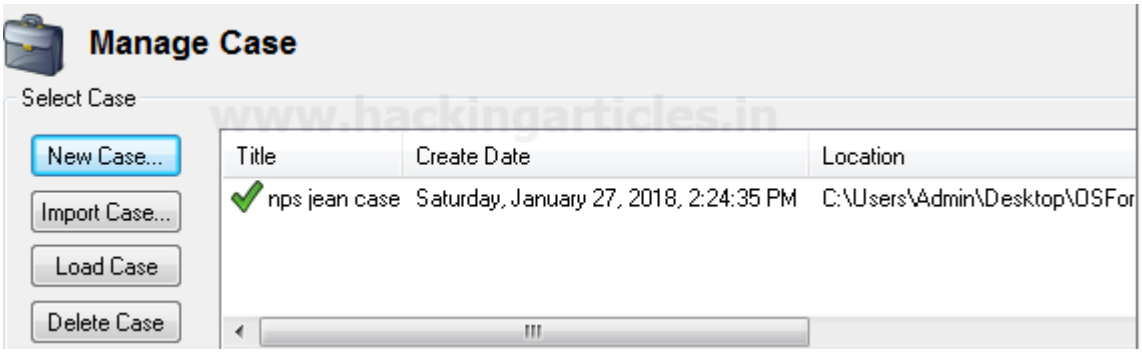
Whatever task/operation we want to perform in OSF, it is always advisable to create a case for that. Creating a case is also helpful to distinguish multiple processes/operations from one another and also act as a container of the work done which is also helpful in future reference.

To create a new case click on the Create Case icon in start option or new case button in Manage case option and provide all the relevant details related to the case. Also, note the location where we want to save the case.



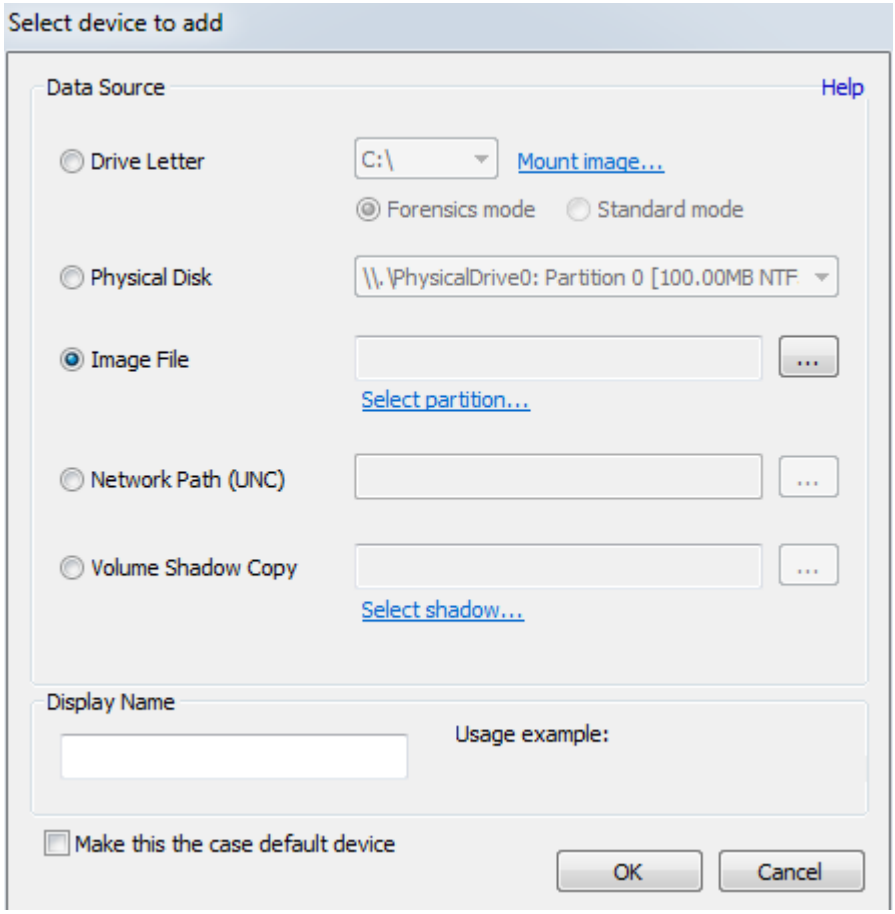
Enter all the details and click on OK, we can see the case getting listed. If are working on more than one case at a time or we have multiple cases listed on OSF we need to select which case we need to work on. To do this select the case and click on the load case, we will see a green check mark against the case which is presently loaded.

We can delete any case or import a case from an already created case.

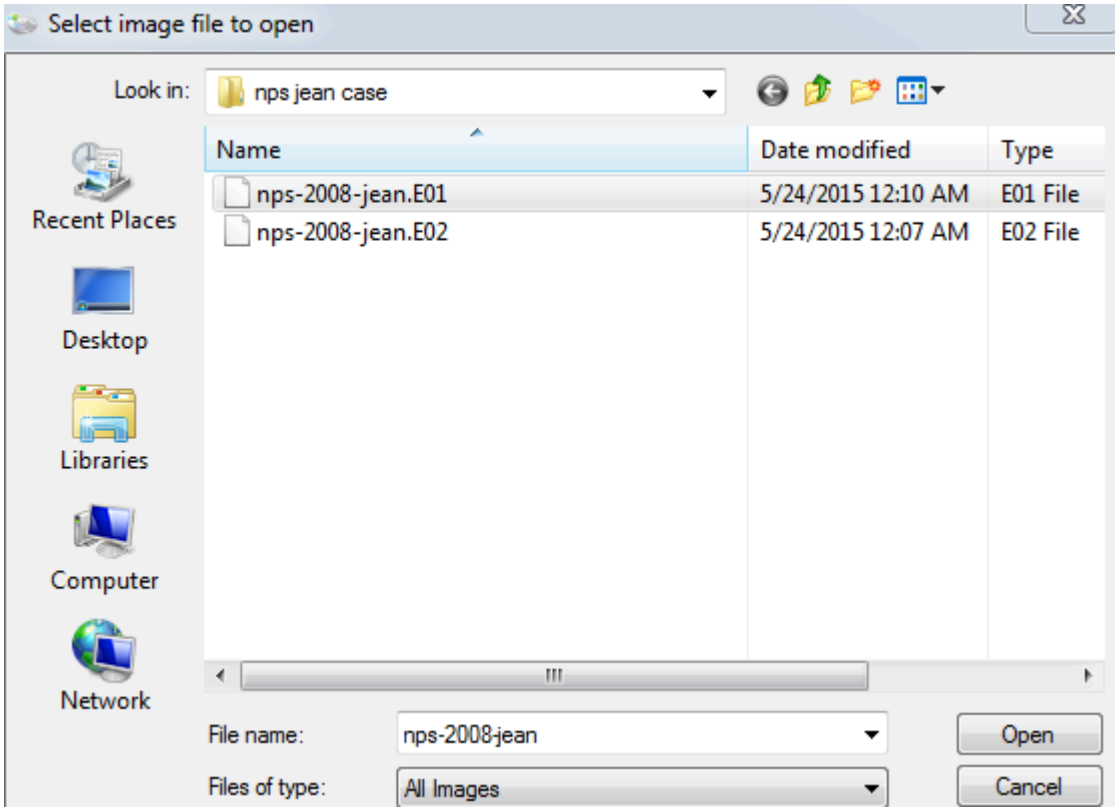


For this article we will be working on NPFJeane case, it is a demo case (E01) of which we will be doing forensics investigation. (This will be our evidence, we can do the same with any other data or computer disk).To

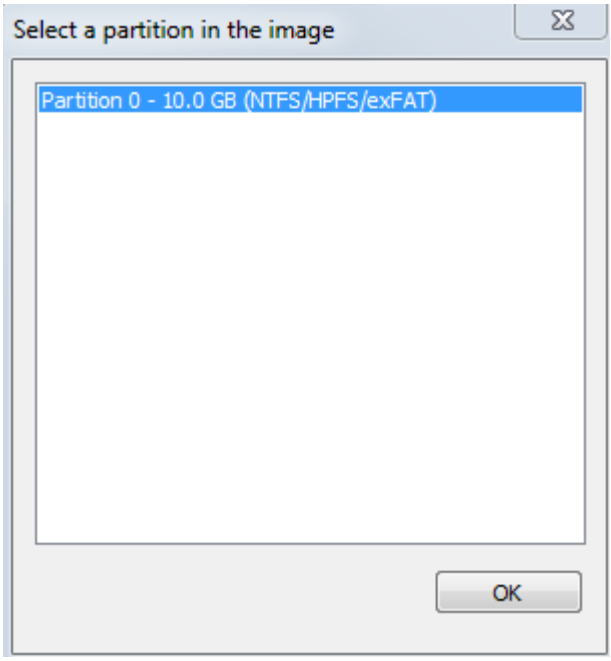
add the evidence to our case click on add device.



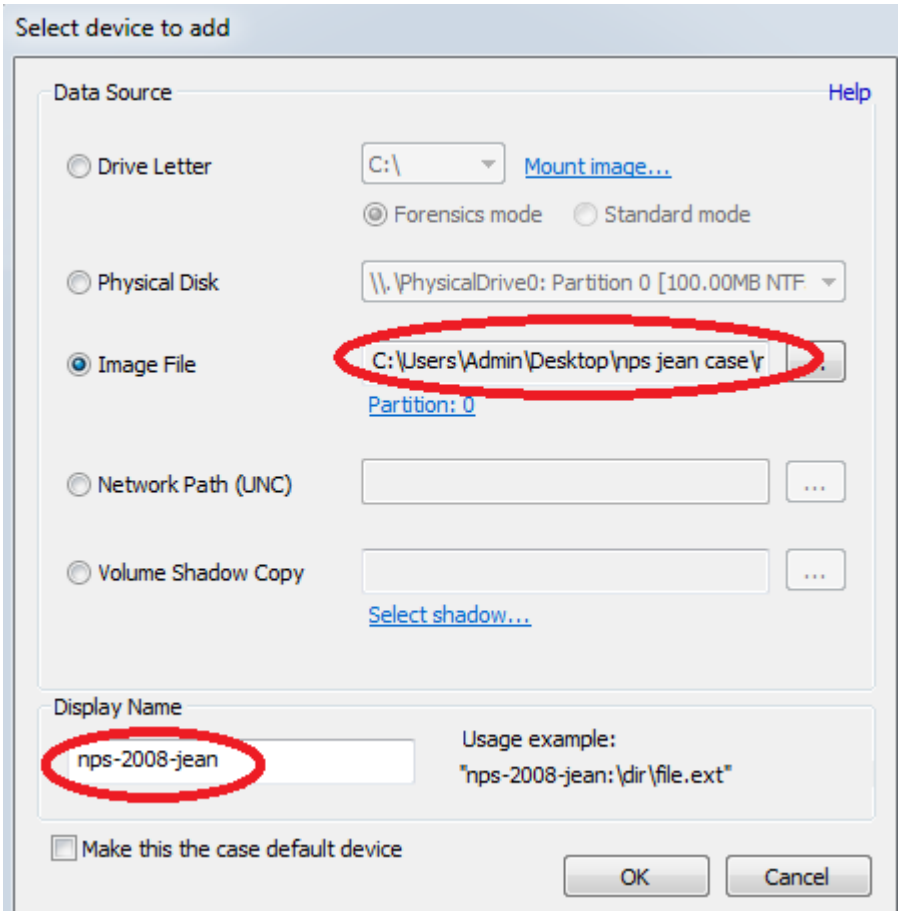
Select the image file and browse for the Evidence file and click open.



All the partitions in the acquired image will get listed. Select the partition and click OK.



The evidence will get added and evidence name will get displayed. If required we can change the display name.



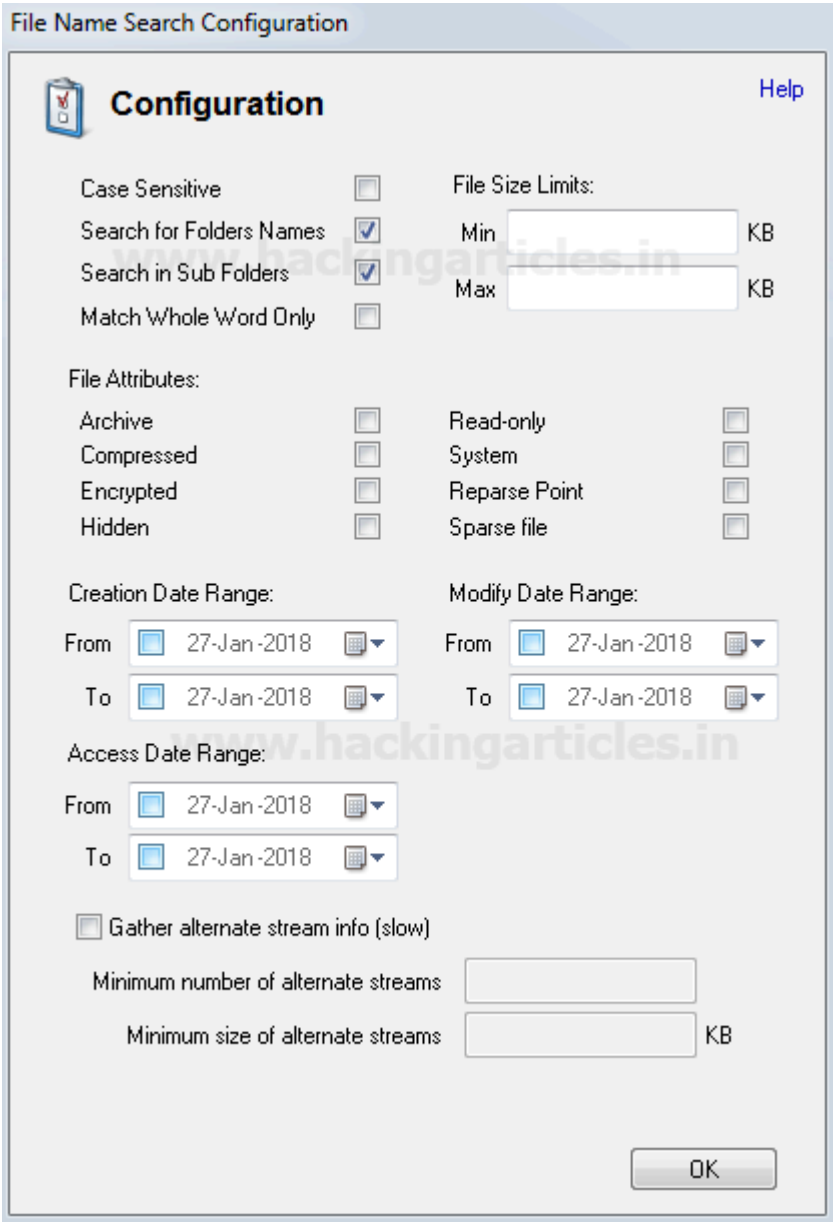
Once successfully added the evidence will get listed as shown below.

File Search

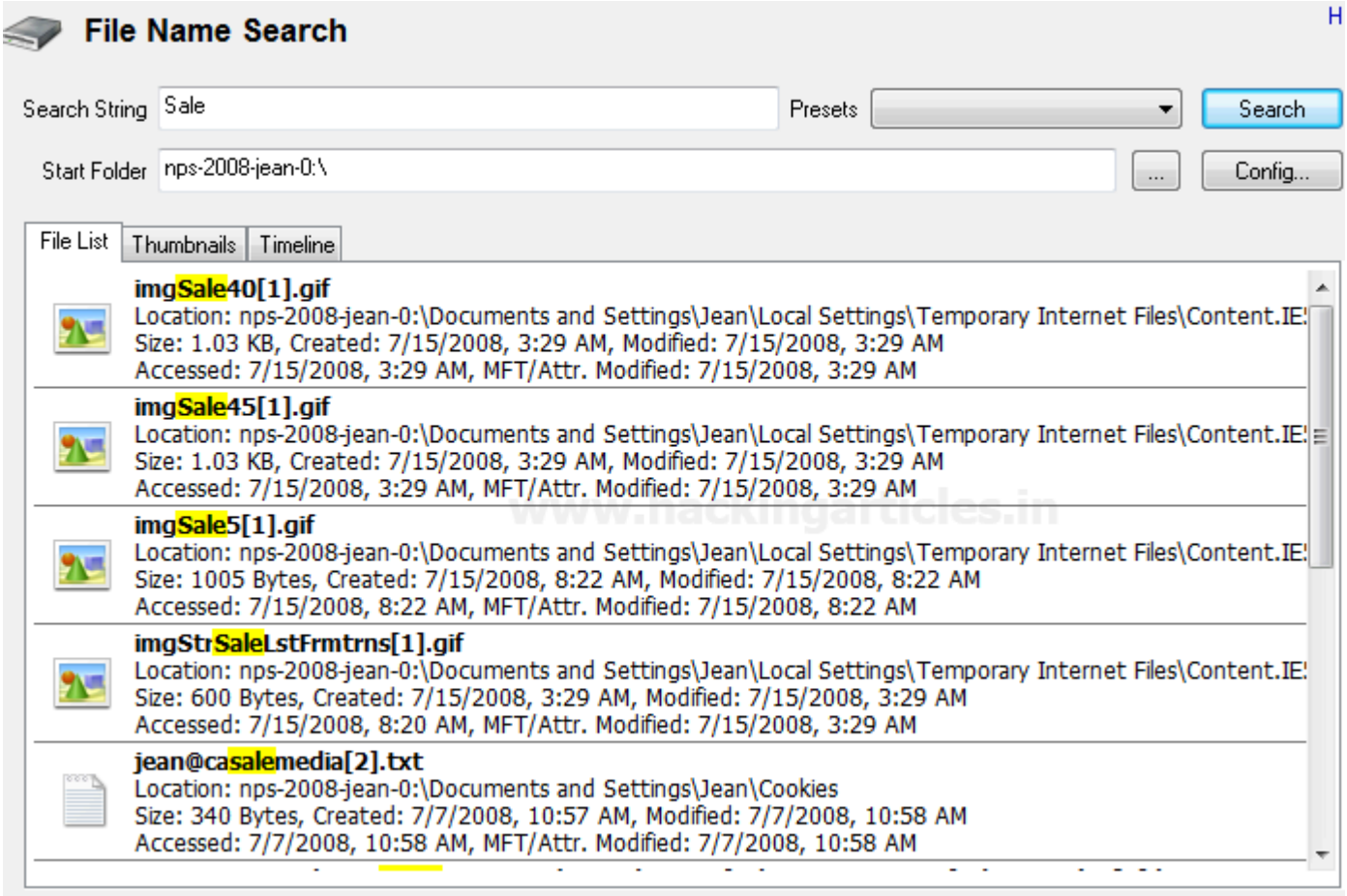
This option is used to search any particular file name, to search any particular file we can simply give the file name and browse for the drive, directory or any other location we need to search.

There is a preset option we can use this to select any particular file category

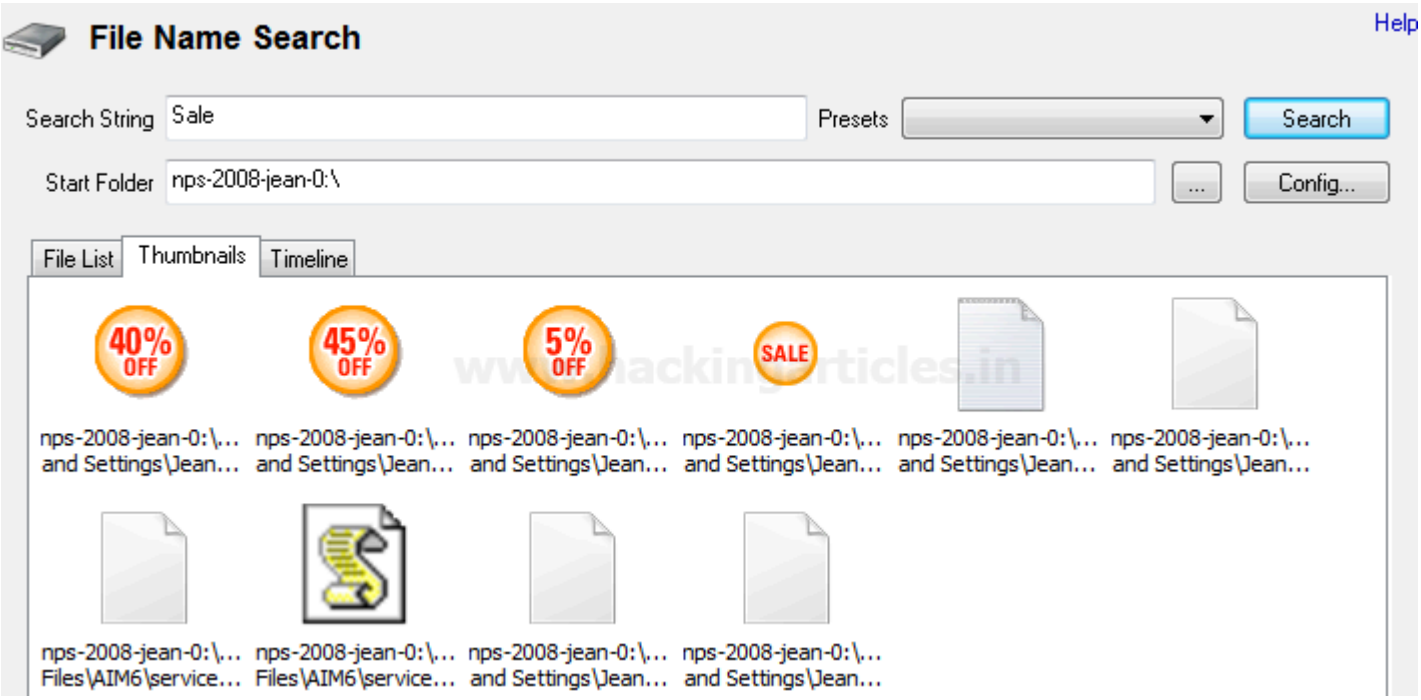
Also, we can filter/refine the file search by changing the configuration settings, to do so click on the config button and change the settings as required.



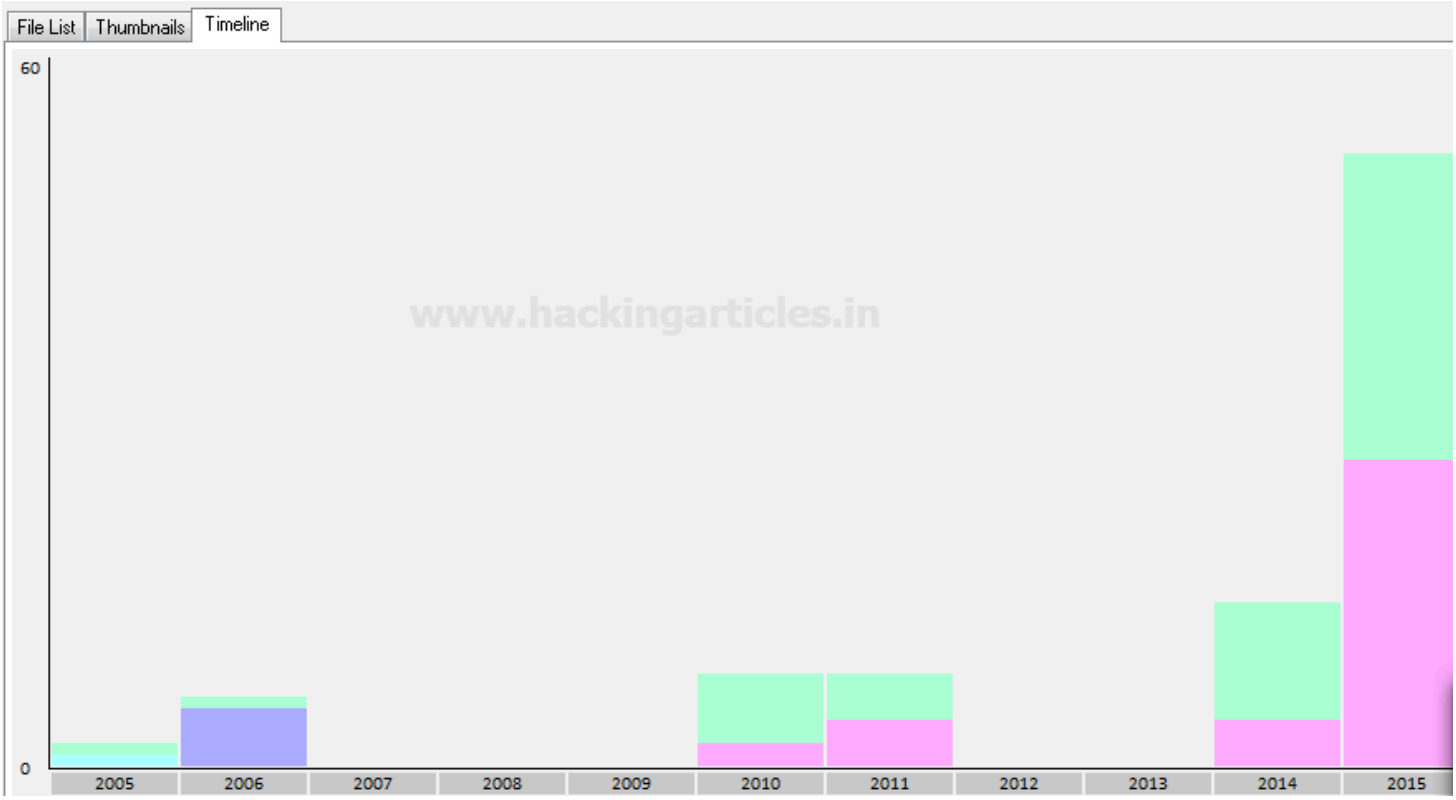
Click on OK and in file search window enter the filename and click on search, Depending on the data volume The search will take a little time and will display the results. In our search, we have searched the term “Sale” and this will show all the files who have the term “resume” in their name.



We can also view the searched files in thumbnails



And timeline view. Timeline view will show a bar graph representation of that keyword on the basis of time and keyword count.

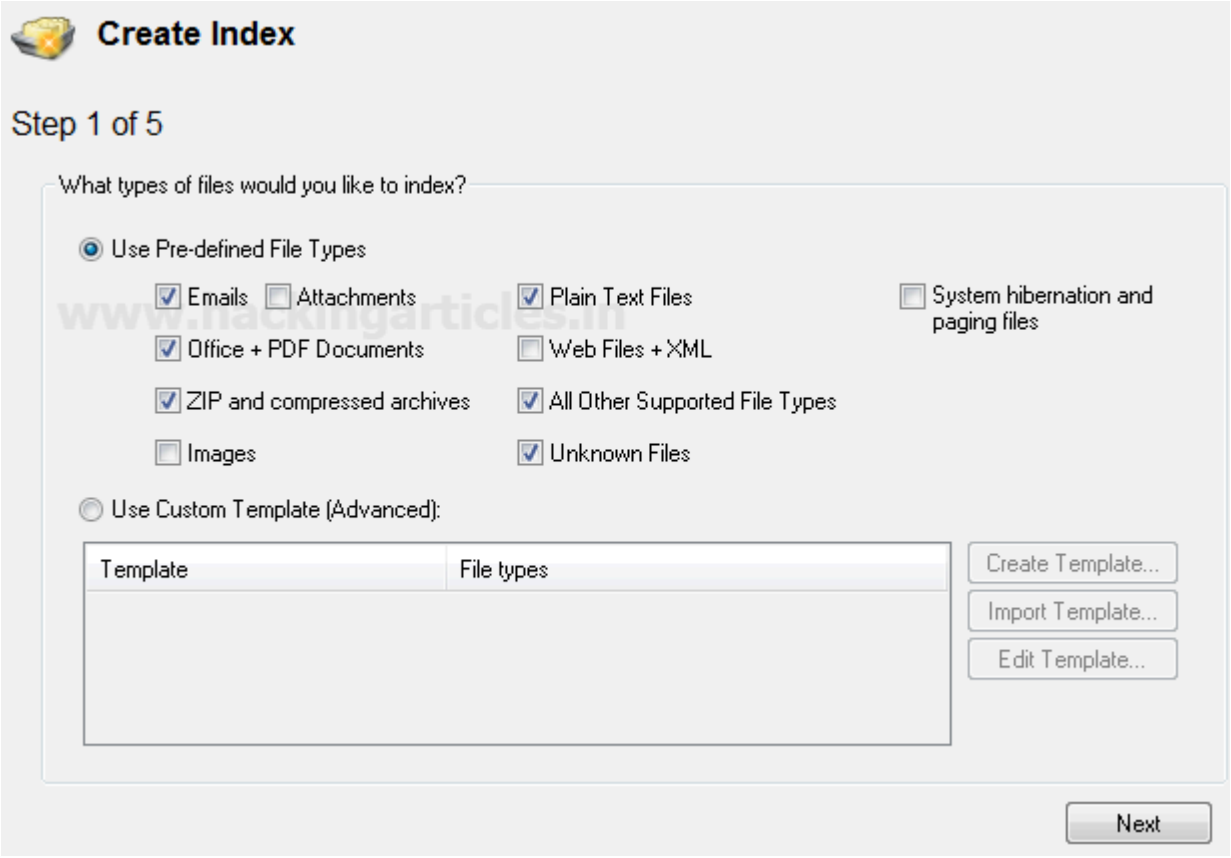


This ends the file search.

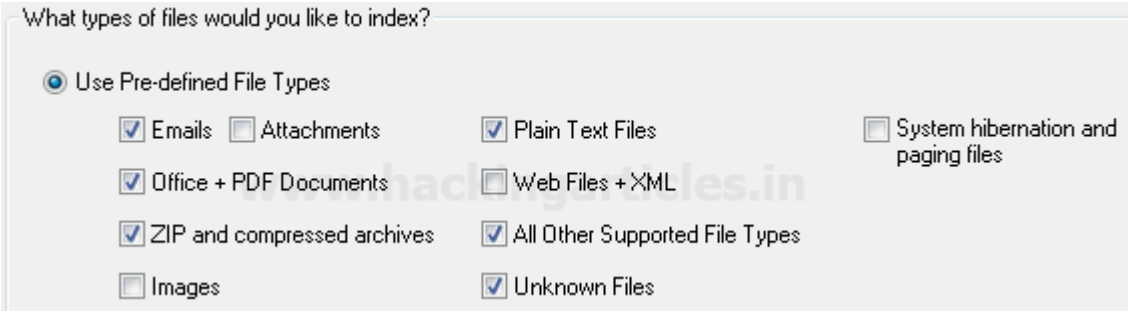
Create Index / Indexing

Index search is a more deep and refined search and also very vital for forensic investigations.

The most intuitive method for keyword searching is to provide a single keyword and search for the occurrence of that keyword within our data/evidence. To achieve this objective the best way is to create an index of the drive/directory within which we need to perform a search. An index is simply a list of offsets for occurrences of required keywords. Indexing allows searching within the contents of many files /drive/directory /image file at once.

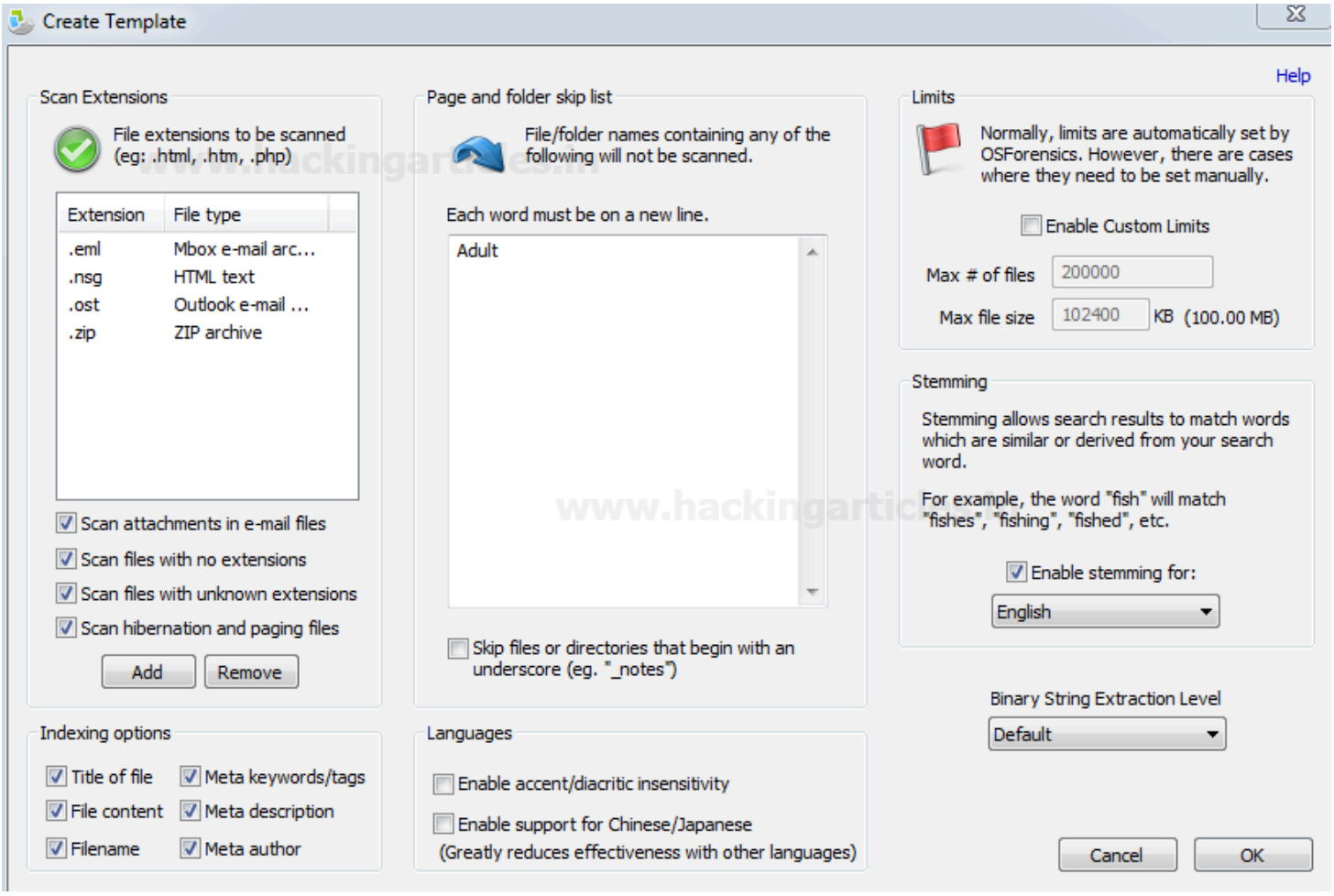


In OSF we can either be indexed on the predefined files types

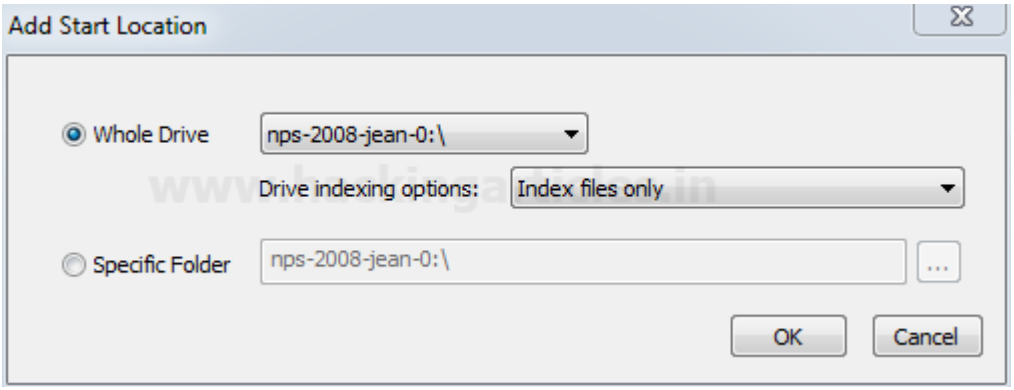


Or can create a customized template

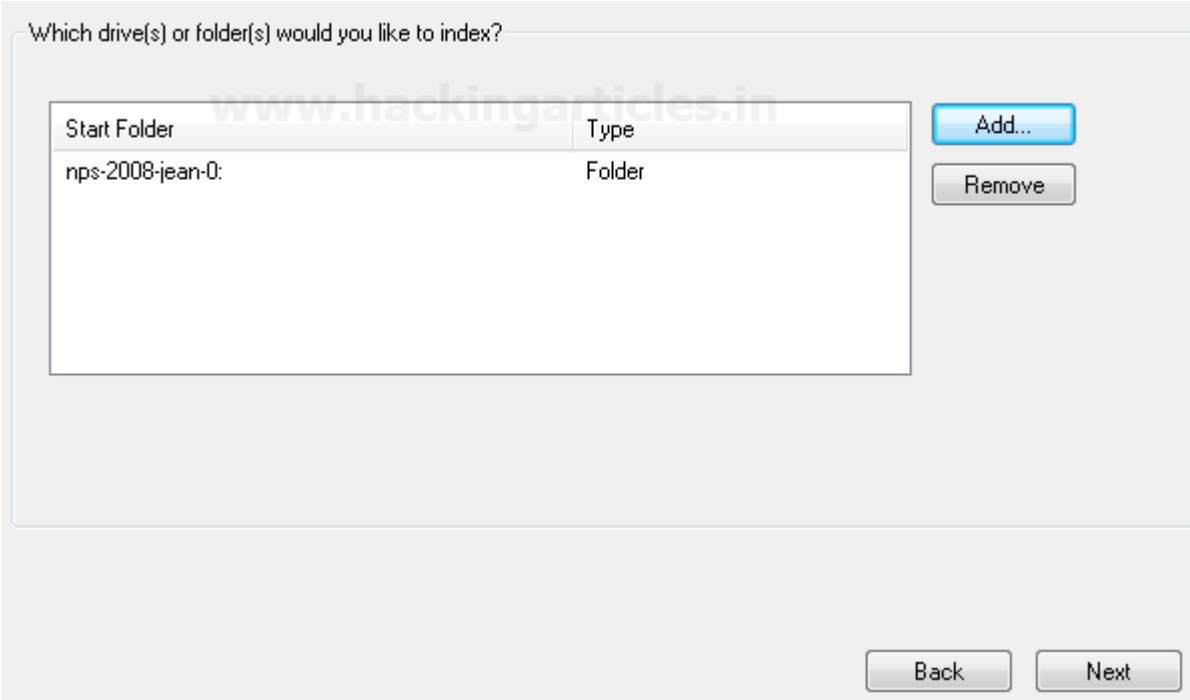
We can select the extensions we need to search on, skip any file or folder by specifying its name or by limiting the file size. Customize the template and click OK



Customize the template and click OK. Click on next and proceed to Step 2. Here we need to select the drive or directory we want to index and select the indexing option from the drop-down as shown below and click on OK.



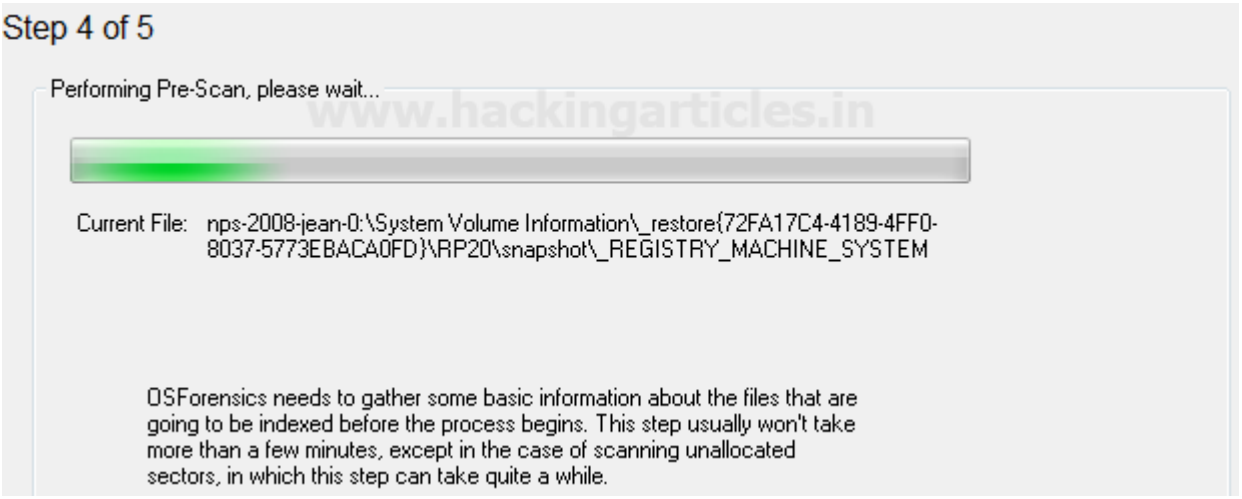
The image, drive or folder selected will get listed, (we can add multiple drives/directories) for indexing.



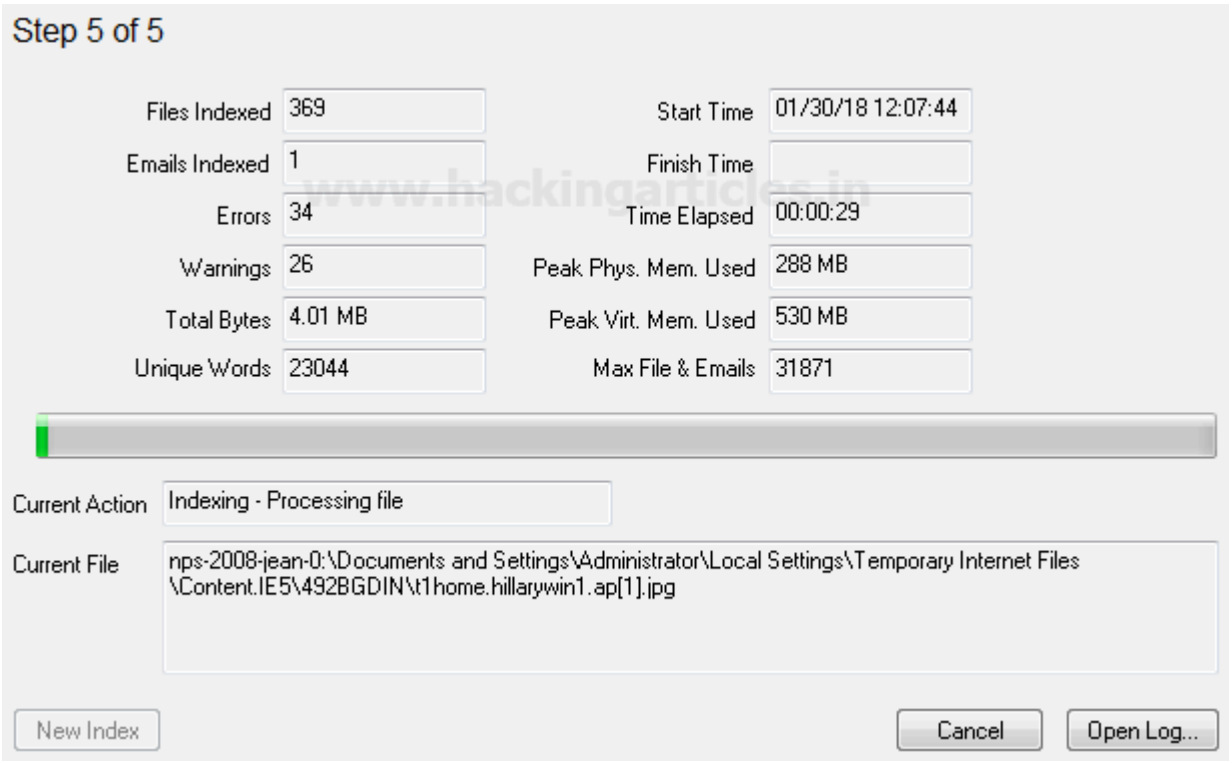
Click on next and proceed to step 3

Now we will get a view of the drives we are indexing along with the extensions that will be indexed. If everything is as per requirement click “Start Indexing” else click the “Back” button to make any changes.

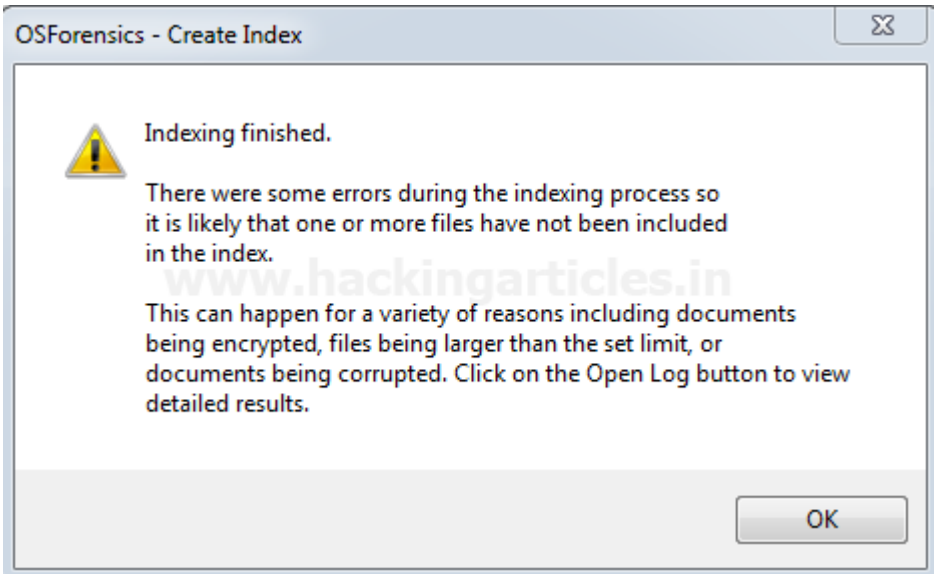
Indexing will start and depending on the data it will take some time for the indexing to complete.



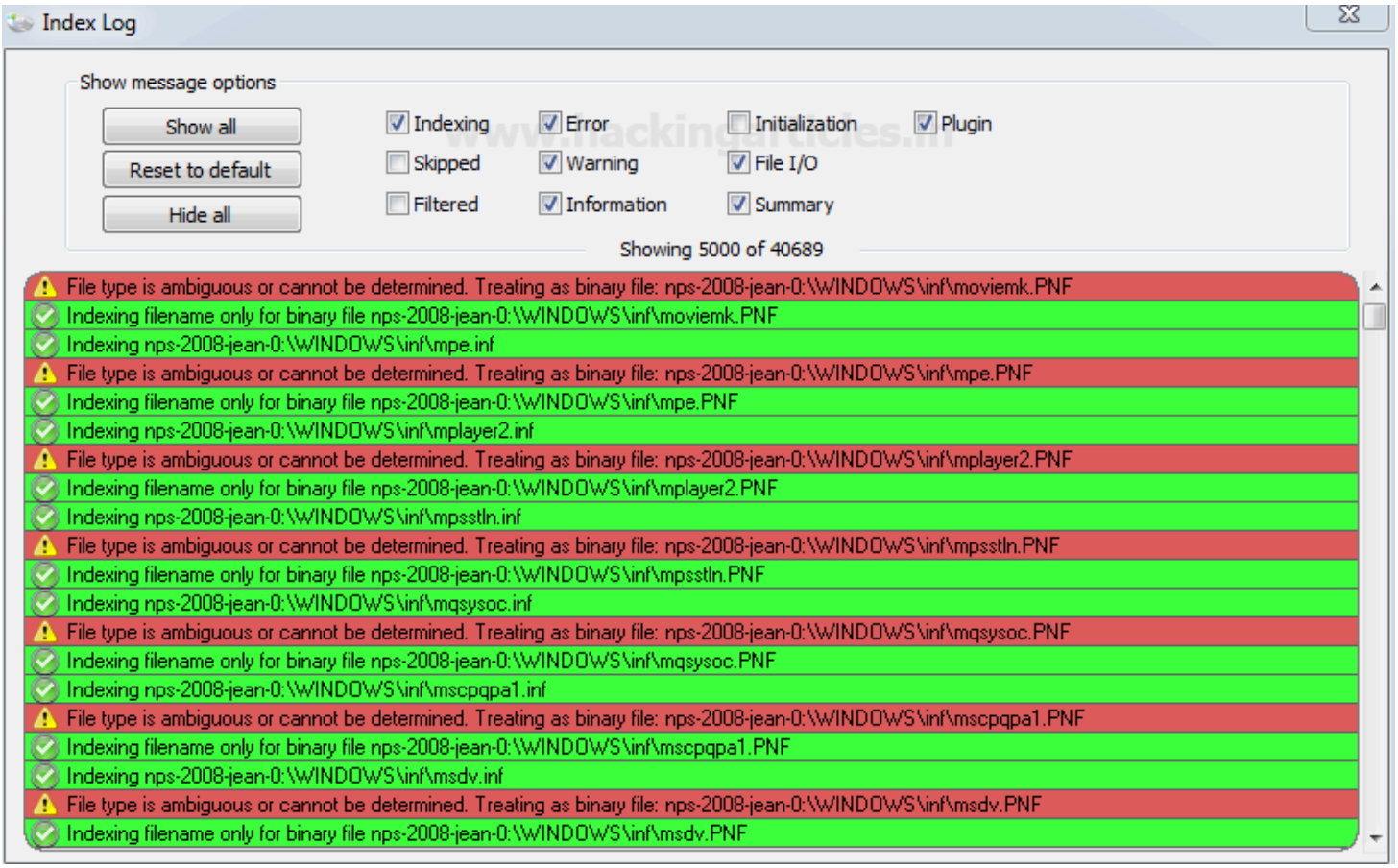
Initially, Prescan is performed and immediately after Pre-Scan indexing will start automatically



Once indexing is complete, we will get a pop up with indexing finished message.



We can also check the index log to check the status /result of indexing and any error that the system may have occurred during indexing.

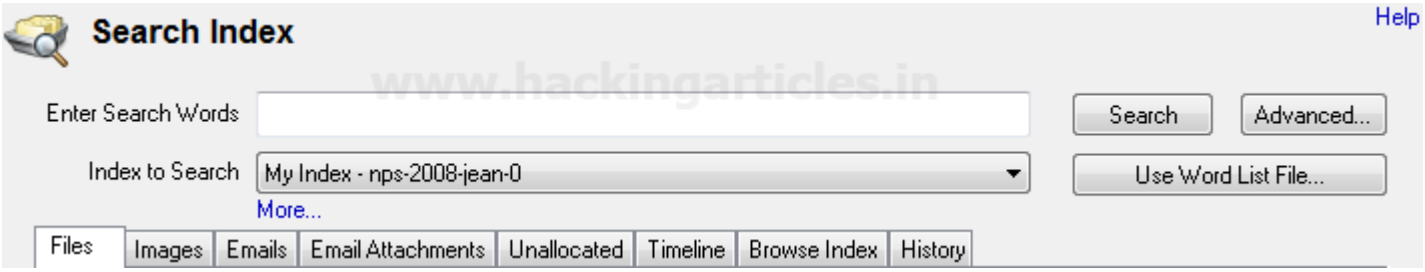


Search Index

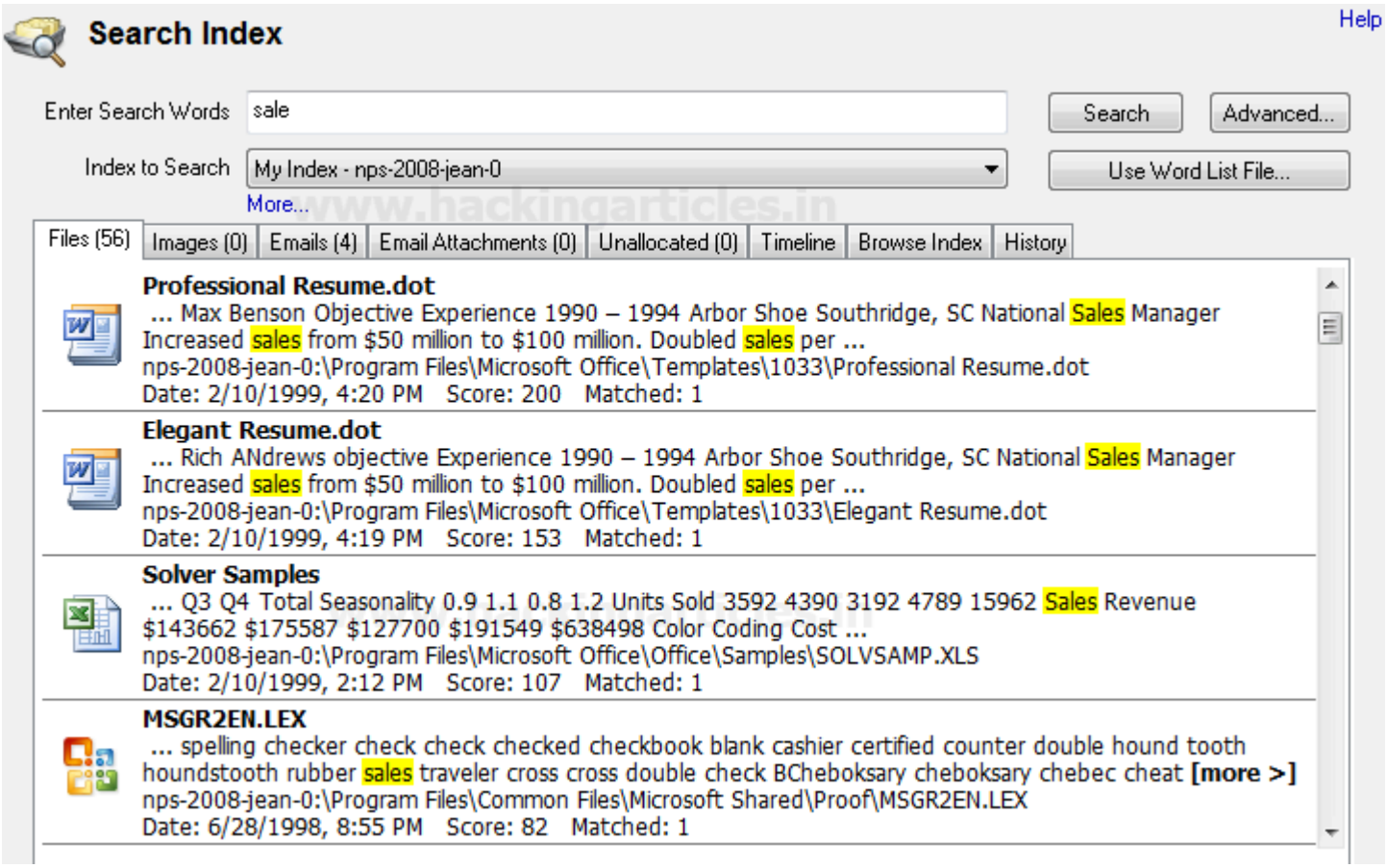
Above we have indexed the drive for keyword searching, now we will actually search for the keywords in the indexed drive/directory.

To start with click on the search index.

We can see all the drive we have indexed in a drop down

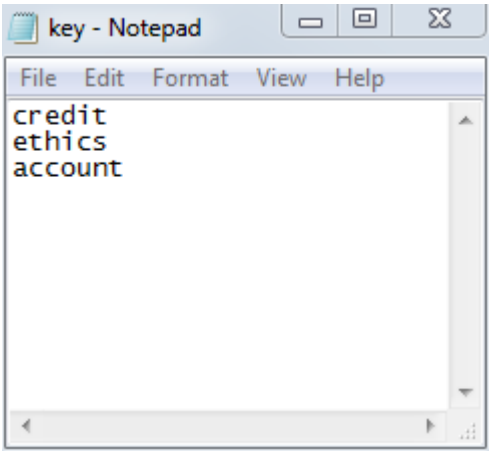


We can either enter the keywords we want to search one by one in the "Enter Search Word" tab click on search and will get the result on the screen. We have searched for the keyword "Sales", inside our evidence and can see all the files containing the word Ethical.



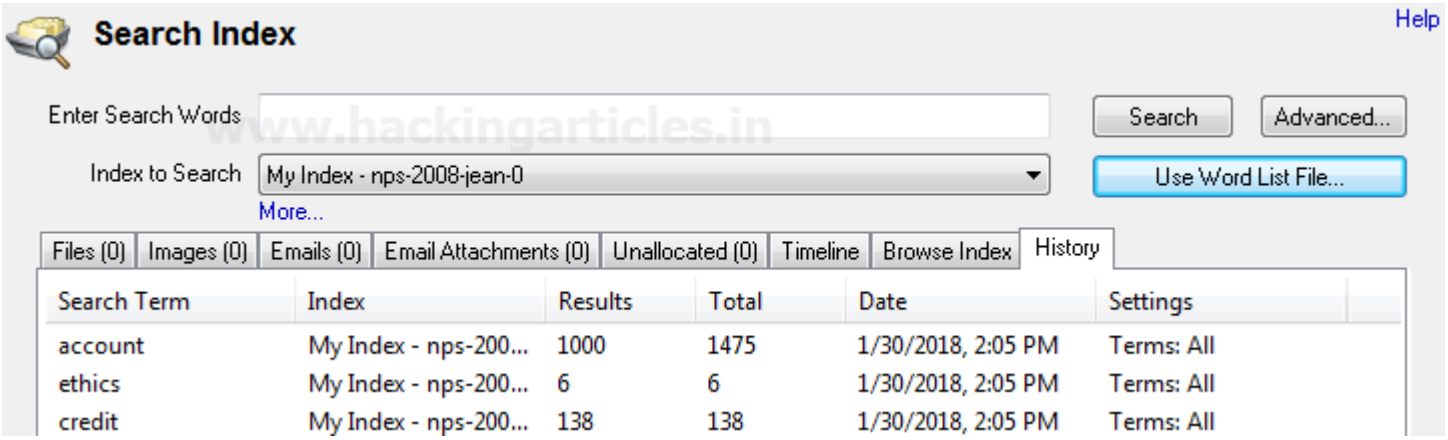
Also, we can upload the keywords we want to search in a text file and upload it, this option is suitable if we want to search for multiple keywords at the same time.

We have created a text file named key.txt with three keywords and saved it on the desktop.

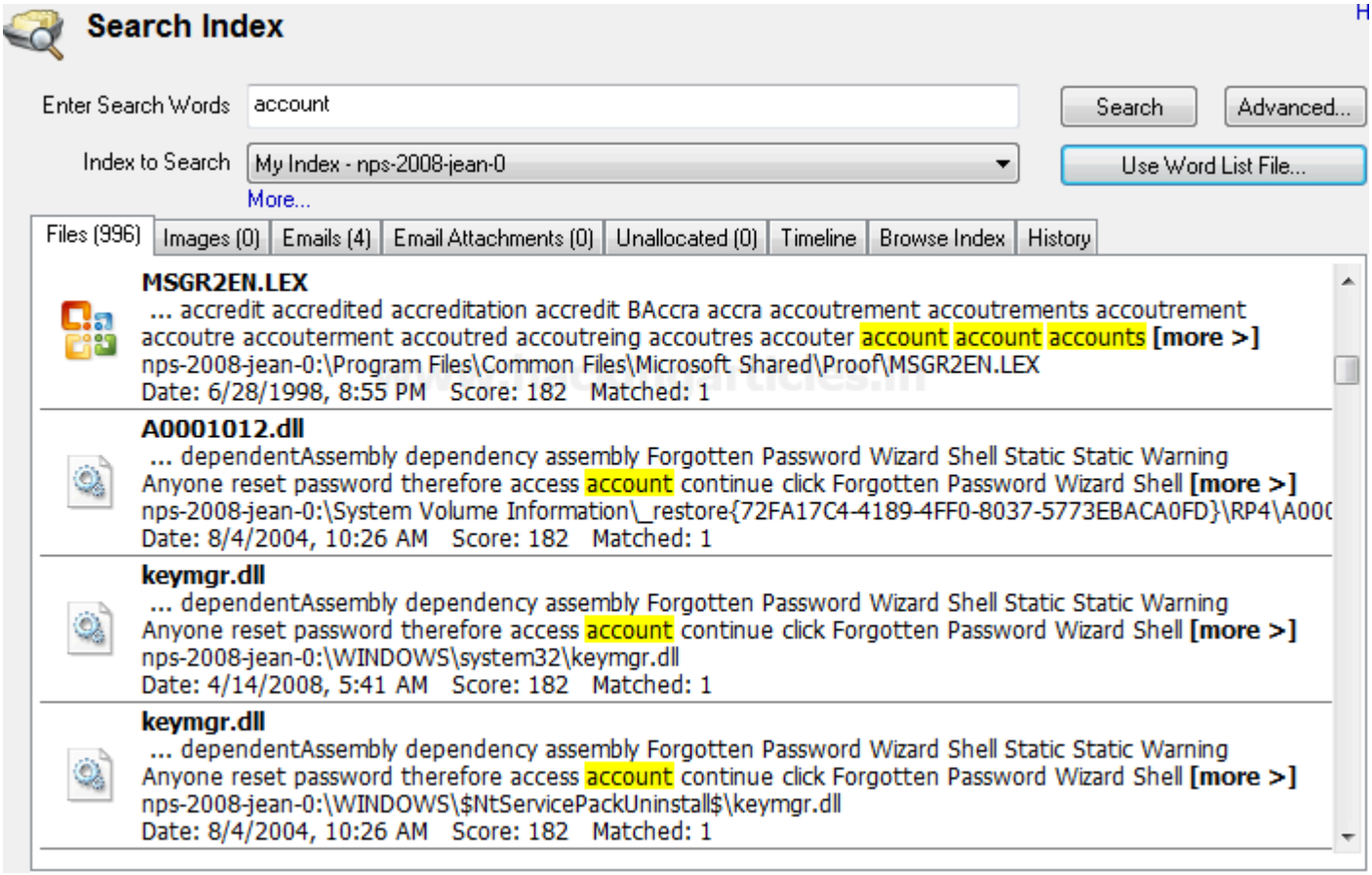


To upload this file click on “Use Word List File” and upload the above-referred file

We can see the result of the keywords in the screen along with the total number of hits of each keyword in the indexed directory, under history Tab.



Double click on the keyword in the list and all the files containing that particular keyword will get listed under the file tab.



This ends the Indexing and searches under-indexing.

For more on OSForensics wait for the next article.