

Digital Forensics Investigation through OS Forensics (Part 3)

February 2, 2018 By Raj Chandel

In Part 2 of this article, we have covered Recent Activity, Deleted File Search, Mismatch File Search, Memory Viewer, and Prefetch Viewer. This article will cover some more features/ functionalities of OSForensics.

To Read Part 2 of this article click [here](#).

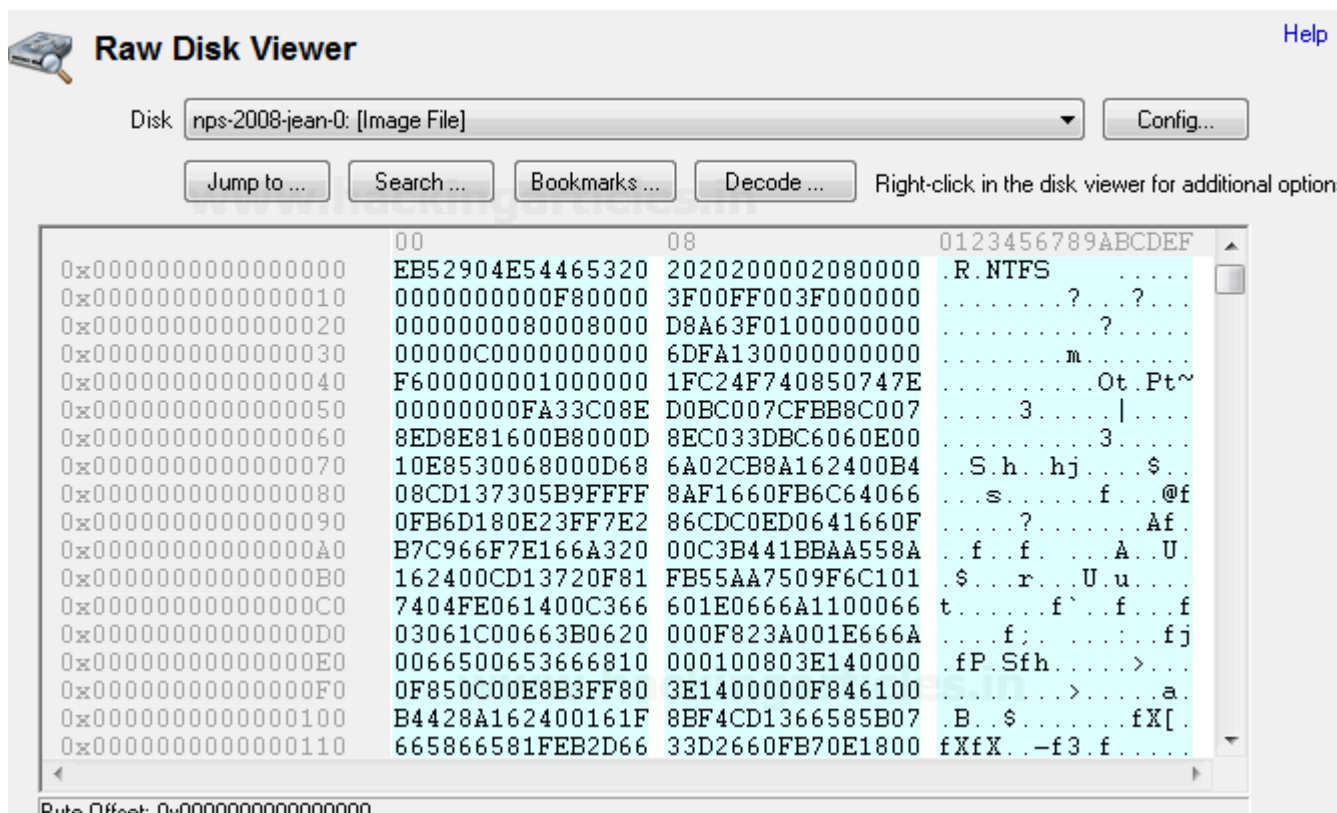
Raw Disk Viewer

On a drive, data is generally stored in file system files and directories but when it comes to forensics we need a deeper inspection of drives we can have a piece of evidence within the raw sectors of the drive, image. These sectors are not accessible through the Operating system but we can access the raw sectors through OS Forensic's Raw Disk Viewer.

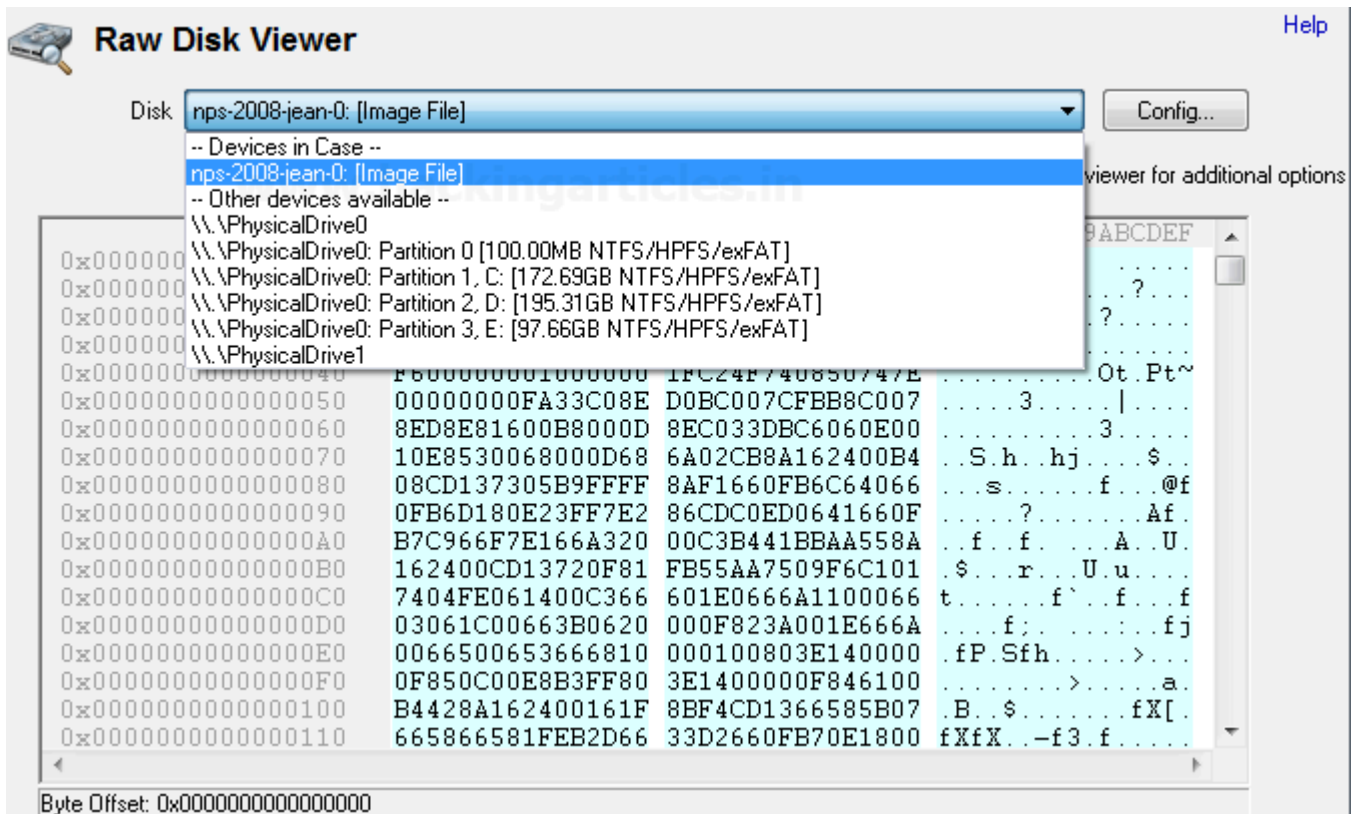
Raw Disk Viewer includes text/hex searching, highlighting of relevant disk offsets, and decoding of known disk structures (such as MBR, GPT)

Source: <https://www.osforensics.com>

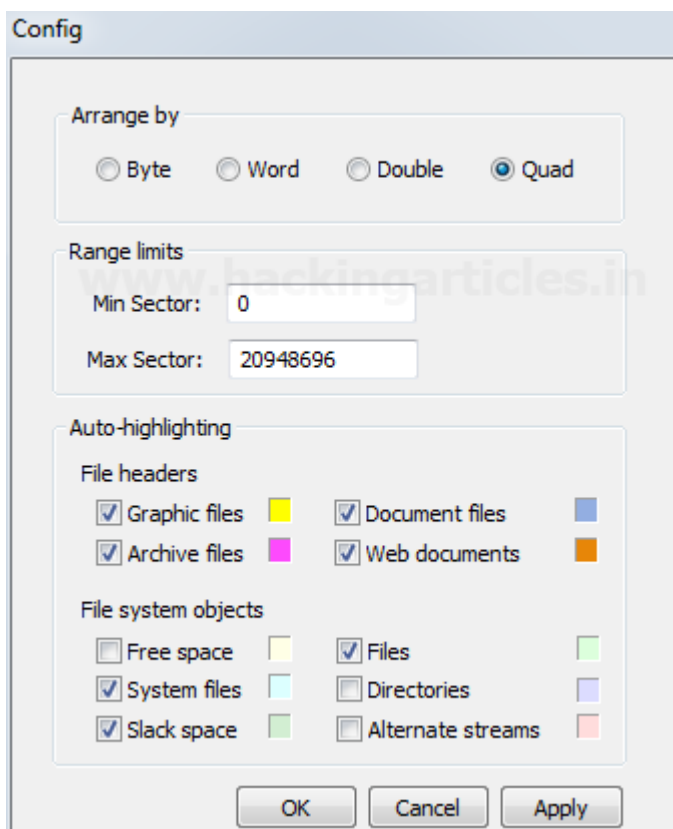
To start with open OSF and click on Raw Disk Viewer



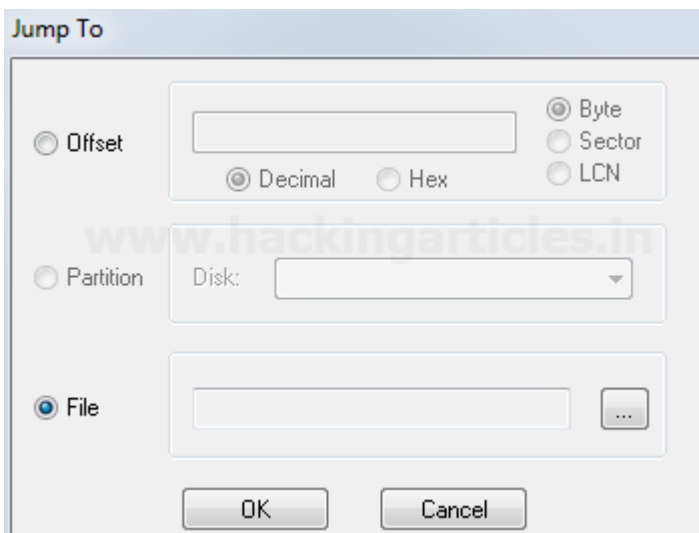
From the disk drop down to select the Evidence we want to investigate.



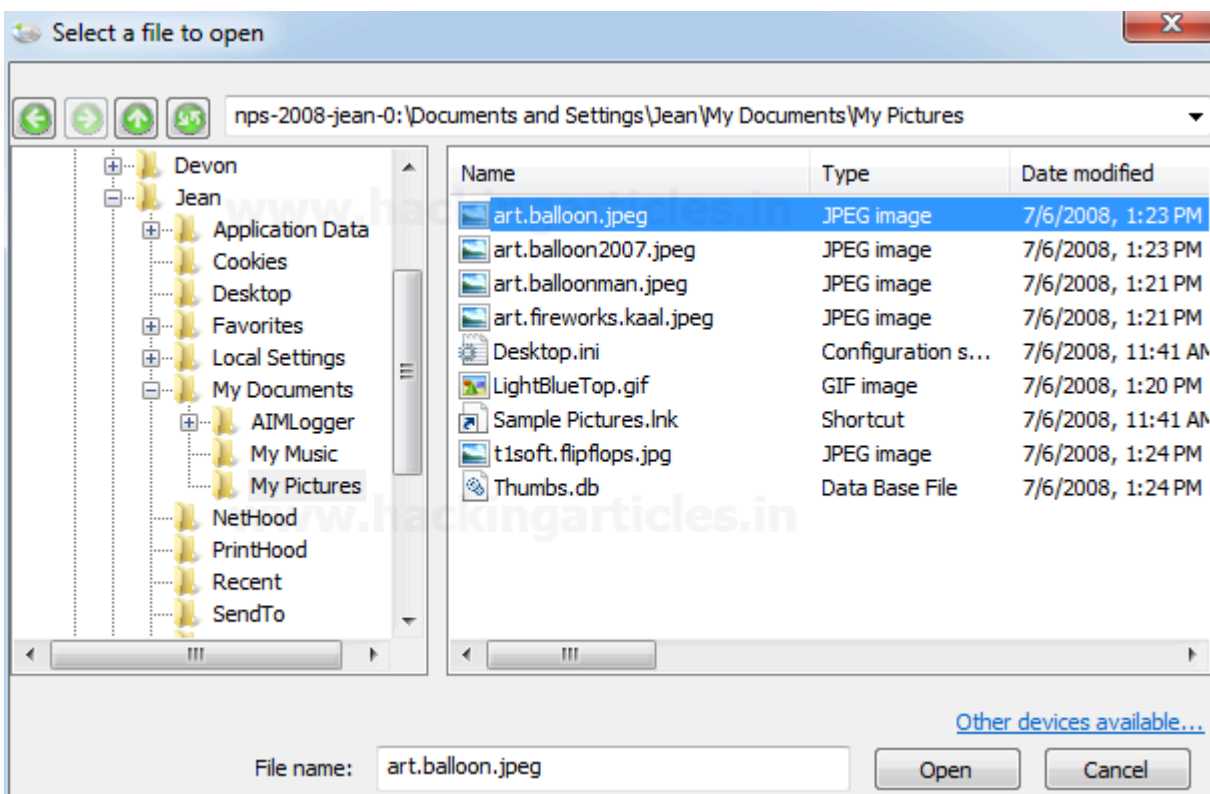
Click on the config button and make the required changes. We can specify the sector range limit, highlight the file types by different colors, include/exclude file system objects.



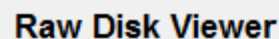
To look for a particular file/sector/offset click on Jump To button, we can see a screen to select any particular file or offset.



To get the details of any particular file select file and browse the file.



Click on open and then OK, the file will open in HEX for investigation.



[Help](#)

Disk nps-2008-jean-0: [Image File]

Config...

Jump to ...

Search ...

Bookmarks ...

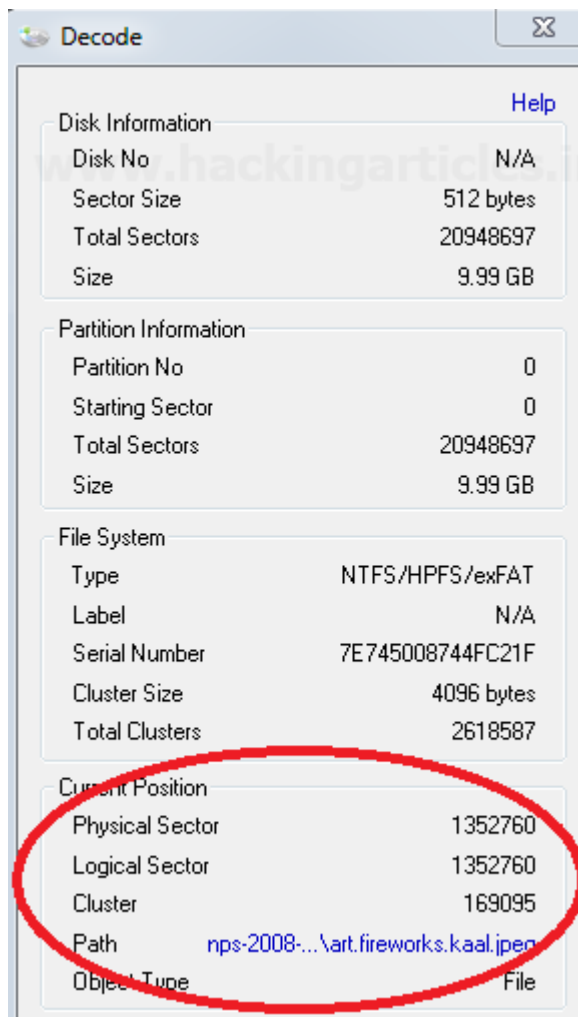
Decode ...

Right-click in the disk viewer for additional options

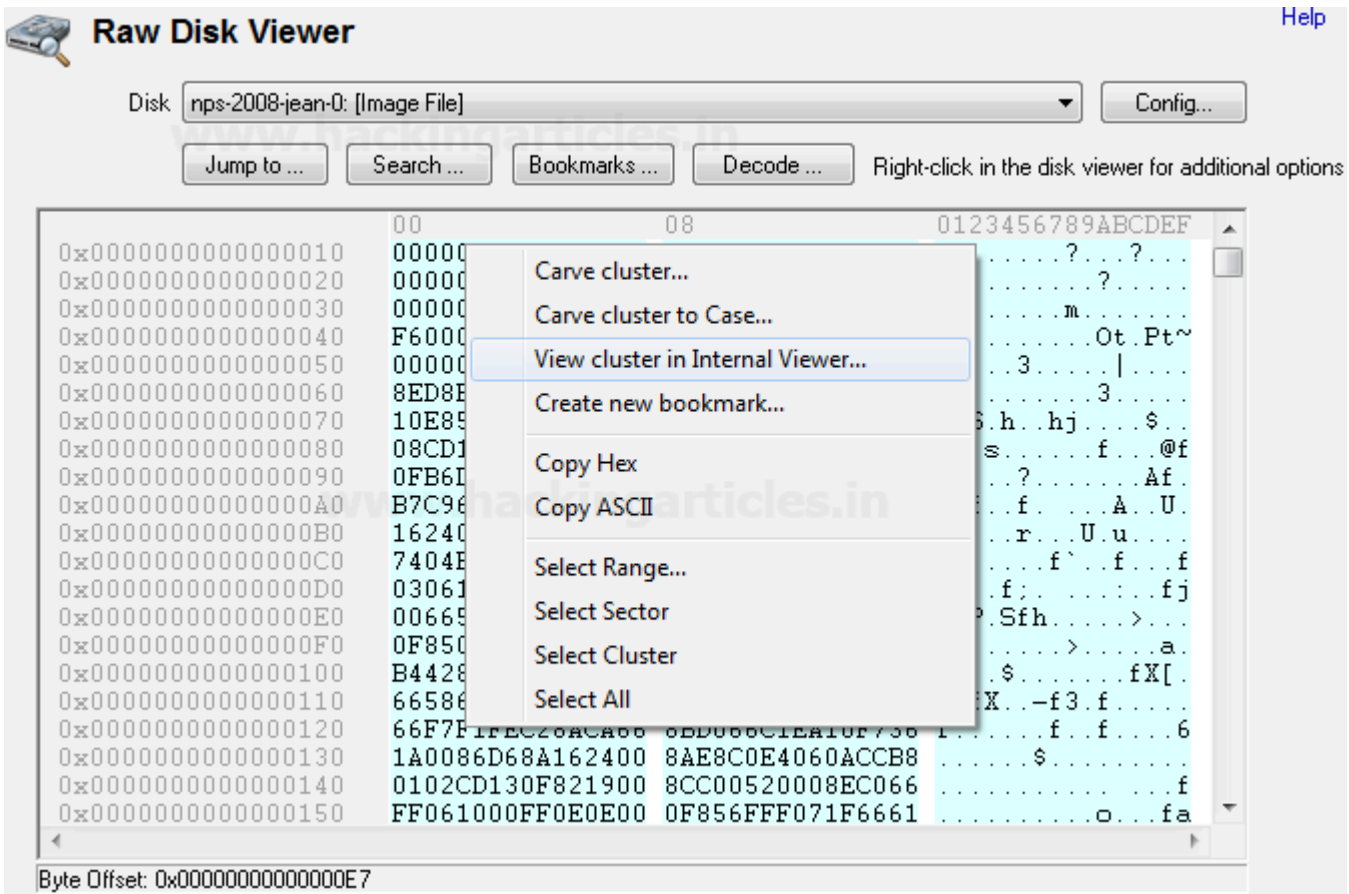
00	08	0123456789ABCDEF
0x0000000000000000	EB52904E54465320	2020200002080000 .R.NTFS .
0x0000000000000010	0000000000F80000	3F00FF003F000000?..?..
0x0000000000000020	0000000080008000	D8A63F0100000000?.....
0x0000000000000030	00000C0000000000	6DFA130000000000m.....
0x0000000000000040	F600000001000000	1FC24F740850747EOt.Pt~
0x0000000000000050	00000000FA33C08E	D0BC007CFBB8C0073..... ...
0x0000000000000060	8ED8E81600B8000D	8EC033DBC6060E003.....
0x0000000000000070	10E8530068000D68	6A02CB8A162400B4 ..S.h..hj...\$.
0x0000000000000080	08CD137305B9FFFF	8AF1660FB6C64066 ...s.....f...@f
0x0000000000000090	0FB6D180E23FF7E2	86CDC0ED0641660F?.....Af.
0x00000000000000A0	B7C966F7E166A320	00C3B441BBAA558A ..f..f...A..U.
0x00000000000000B0	162400CD13720F81	FB55AA7509F6C101 ..\$.r...U.u...
0x00000000000000C0	7404FE061400C366	601E0666A1100066 t.....f'..f...f
0x00000000000000D0	03061C00663B0620	000F823A001E666Af;.....fj
0x00000000000000E0	0066500653666810	0001008030E140000 ..fP.Sfh.....>..
0x00000000000000F0	0F850C00E8B3FF80	3E1400000F846100>.....a.
0x0000000000000100	B4428A162400161F	8BF4CD1366585B07 ..B..\$.....fX[.
0x0000000000000110	665866581FEB2D66	33D2660FB70E1800 fXfX...-f3.f.....

Byte Offset: 0x0000000029487148

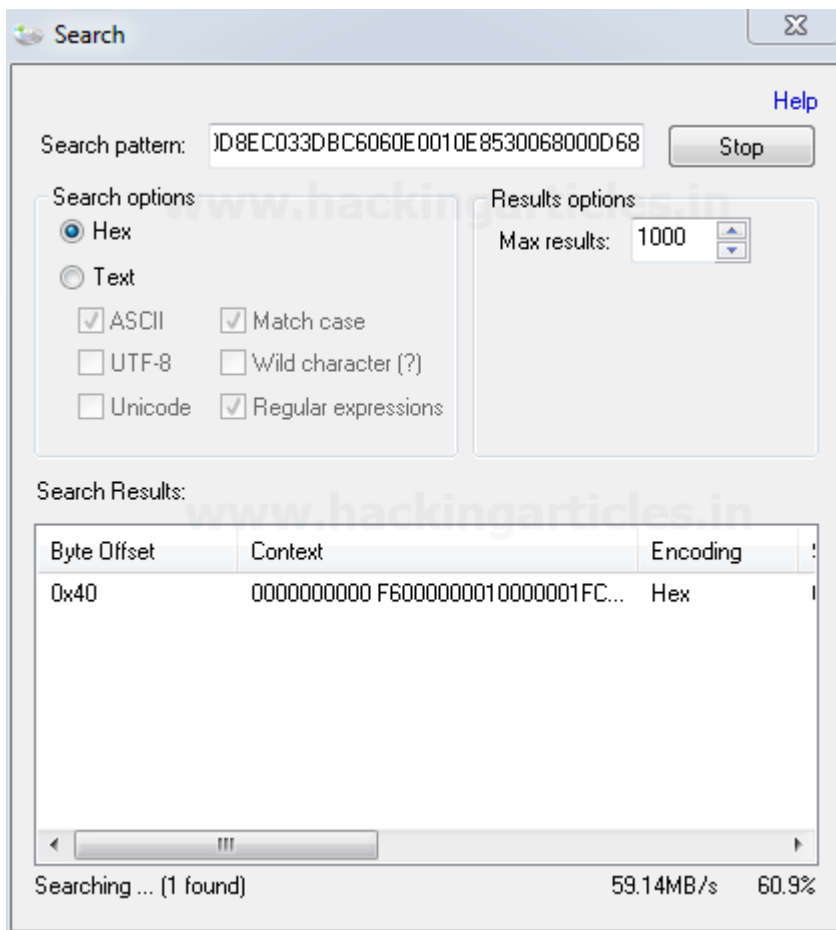
Click on the decode button to get the details of the file. This will provide the cluster number and sector of the file.



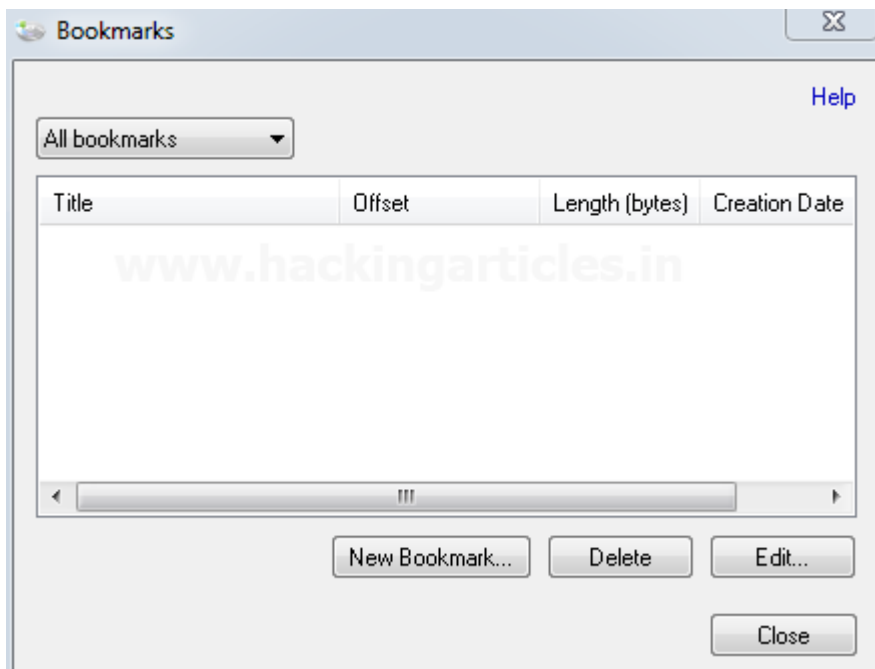
Right click on the file to get all the available options of the file/offset/cluster.



Click on Search button, a screen will appear where we can search for Hex or Text and continue. This will search the particular text or Hex within the raw sectors and will display the result.



Click on bookmark button on the main screen of Raw Disk Viewer. we can create the bookmarks for the relevant evidence.



Create a new bookmark by specifying its start offset and end offset. We can differentiate the bookmark through its color.

Create Bookmark

Bookmark title:

Bookmark type:

Start offset: ☐ Byte ☒ Sector ☐ LCN


End offset: ☒ Decimal ☐ Hex

The bookmark saved will get listed.

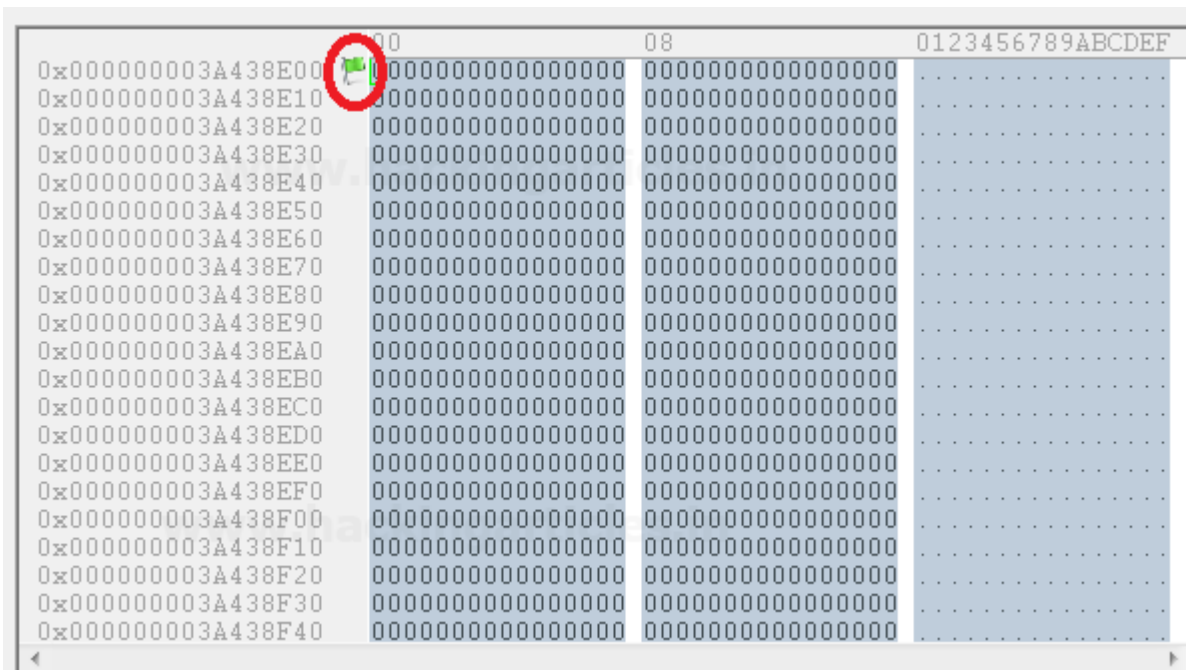
Bookmarks

[Help](#)

All bookmarks

Title	Offset	Length (bytes)	Creation Date
 Bookmark1	0x3A438E00	30208	Thursday, Feb

If we click on the bookmark the offset range will get highlighted on the main screen and will mark the starting of the offset with a flag and color of the flag is that of the bookmark.

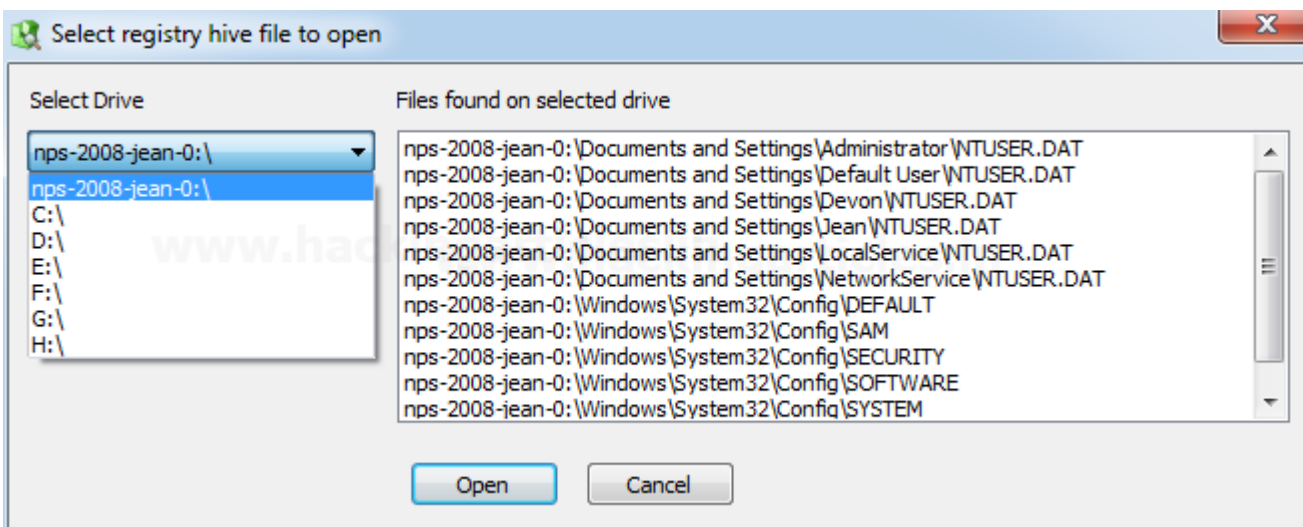


This concludes the Raw Disk Viewer.

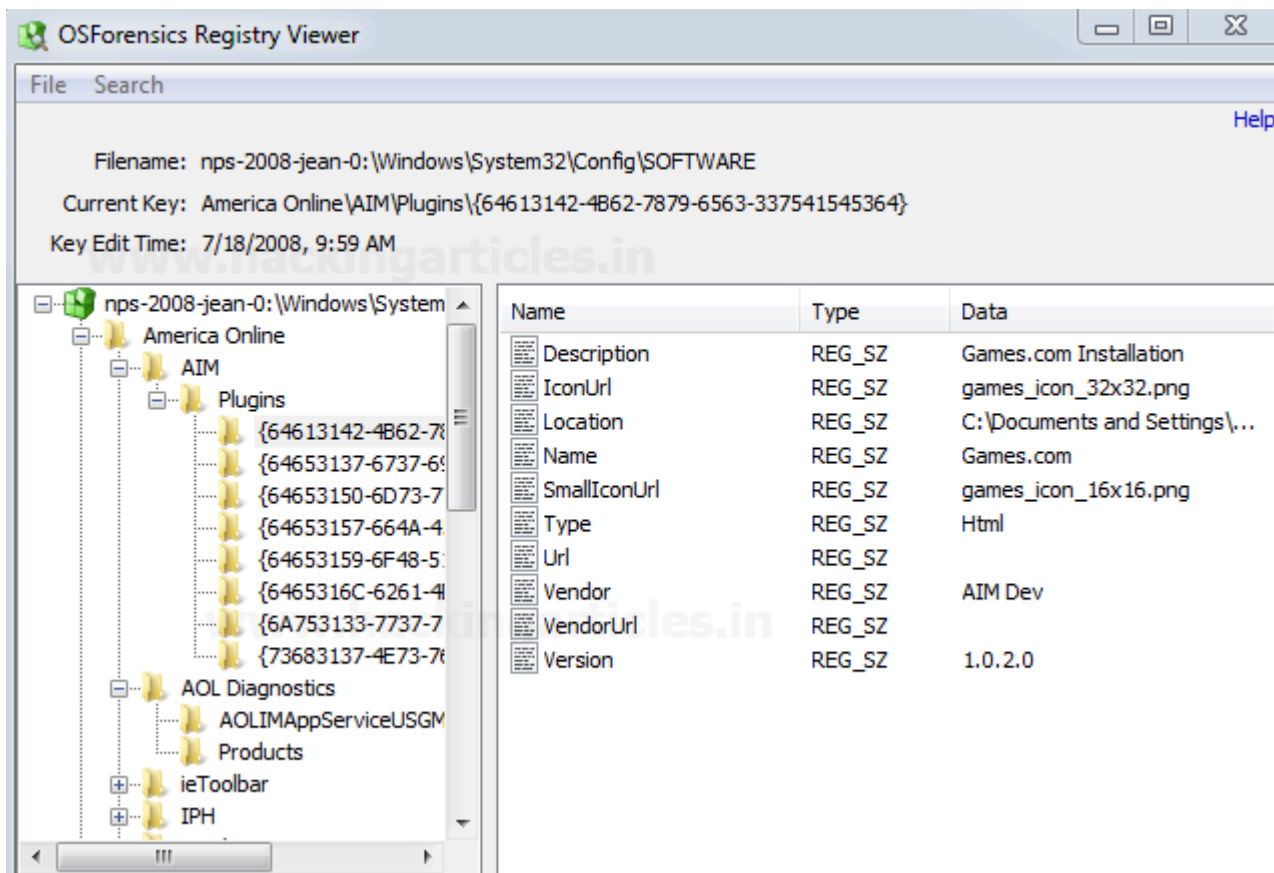
Registry Viewer

Registry viewer enables to investigate the registries of evidence.

To start with open the registry viewer, we can select the drive/evidence we want to work on. All the registry files in that particular drive/evidence will get listed on the right side.



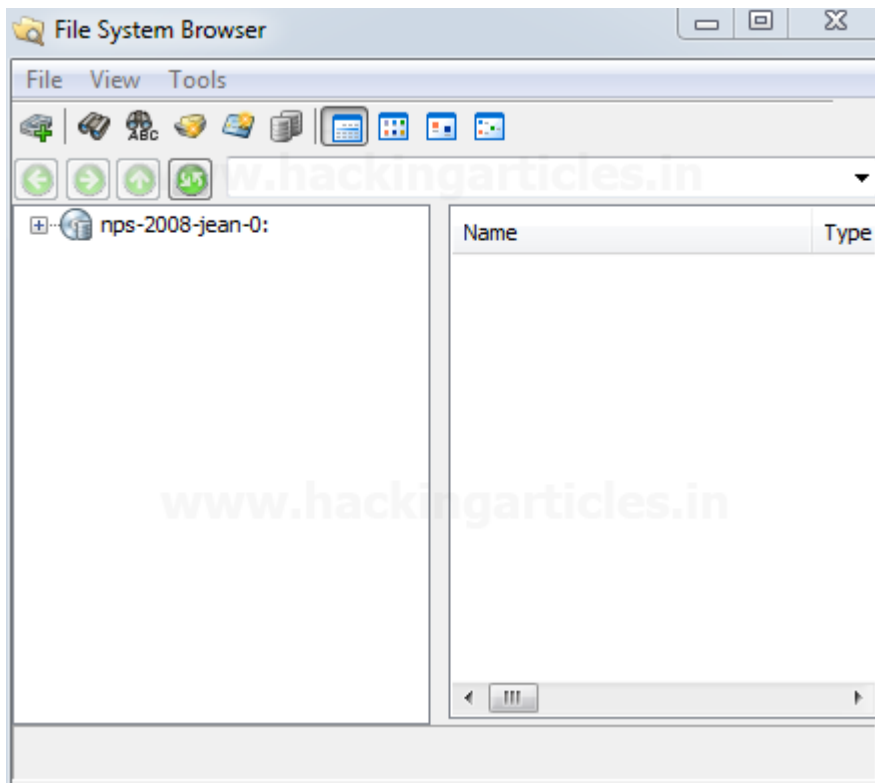
Double Click on any file and we can navigate to the registries and can get all the details.



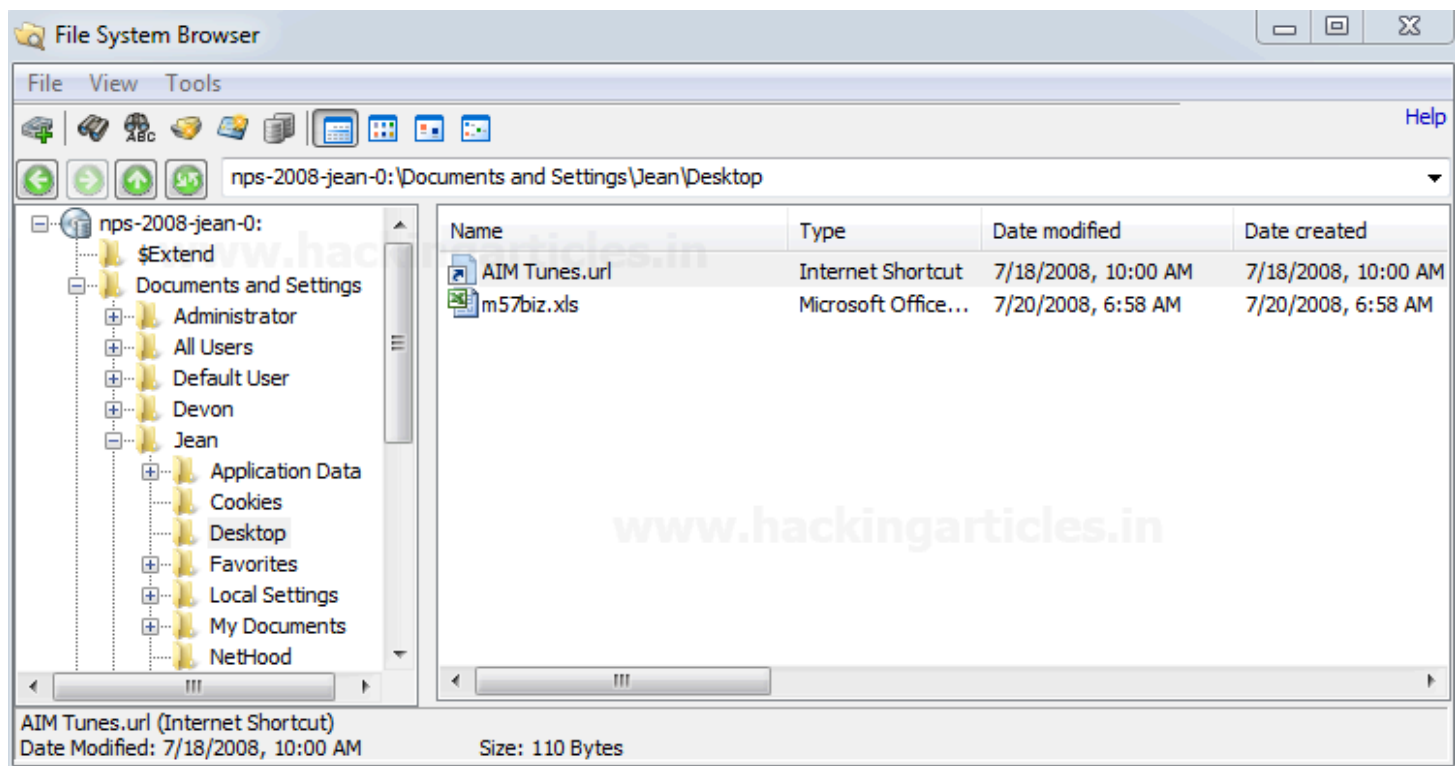
This concludes Registry Viewer

File System Browser

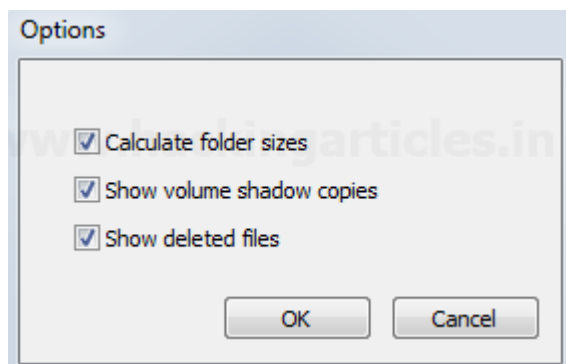
File system browser enables us to navigate to the Drive/Evidence.



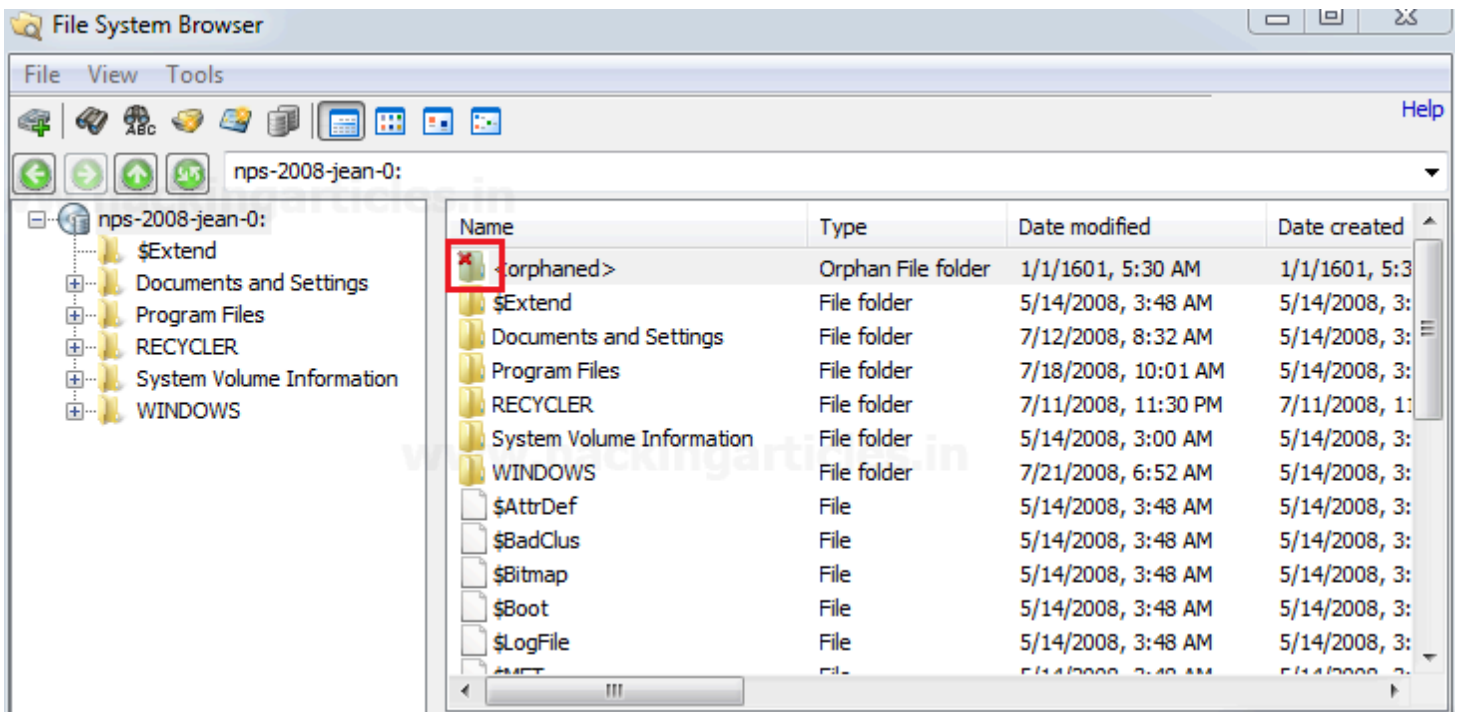
We can navigate through all the files/directories and perform multiple activities. In file system browser we have the other options of OSF as well like File search, Mismatch search, Create Index, Create signature. Some of these features we have already talked about and some of them we will discuss in coming articles.



We can check the “Show Deleted File” option by clicking on Tools > Option > Show Deleted File.



The deleted files/directories (if any) will also get listed and will be marked with a red cross.

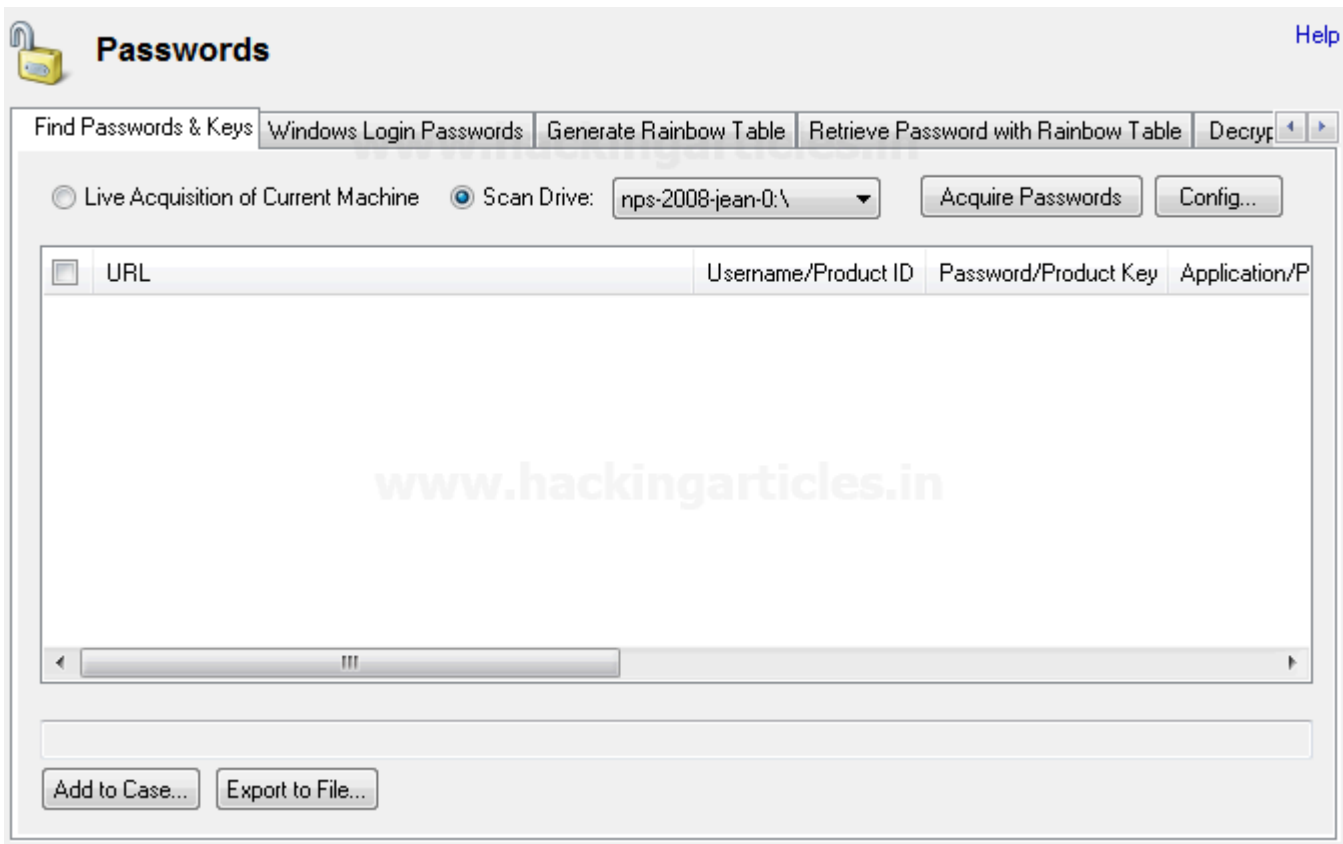


This concludes the File System Browser.

Passwords

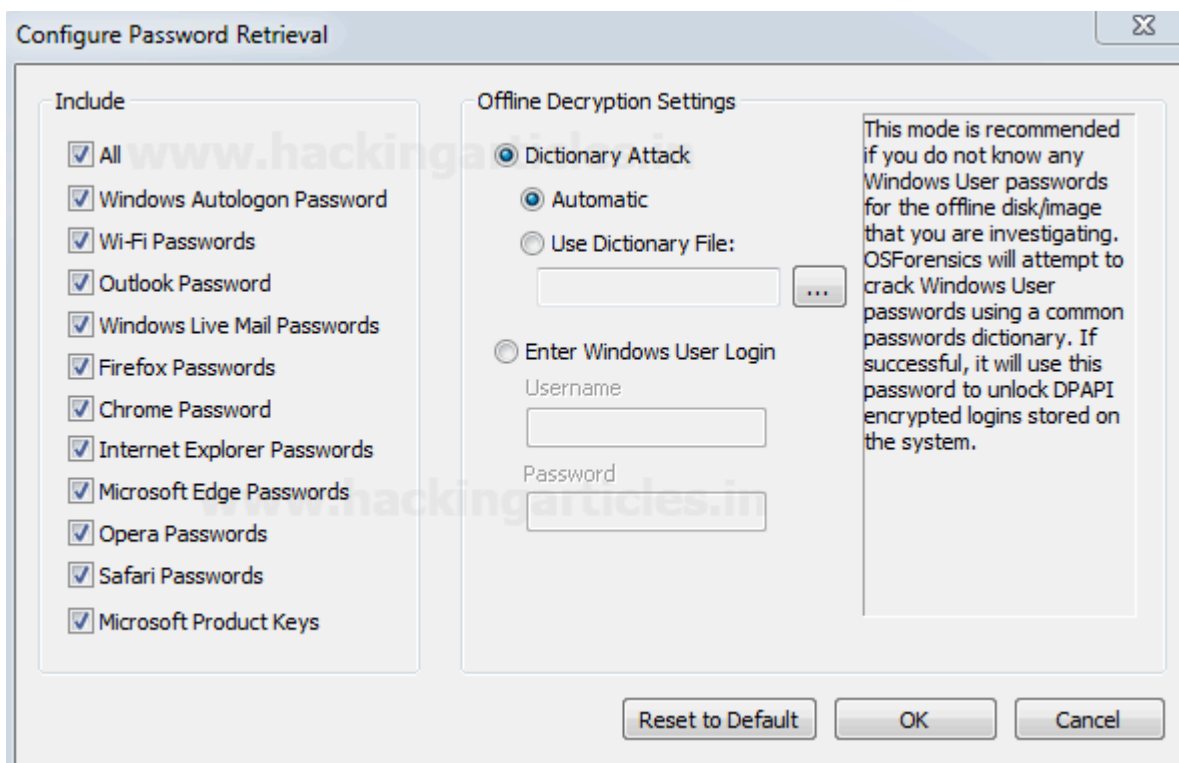
Passwords feature enable us to retrieve the password-related information of the evidence. These passwords could be passwords stored within the browser, Windows Login Passwords, WE can also create a rainbow table by making the multiple combinations of the passwords and retrieve the passwords from the rainbow table. Under OSF passwords also have an option to decrypt an encrypted file.

To start with open OSF and select passwords

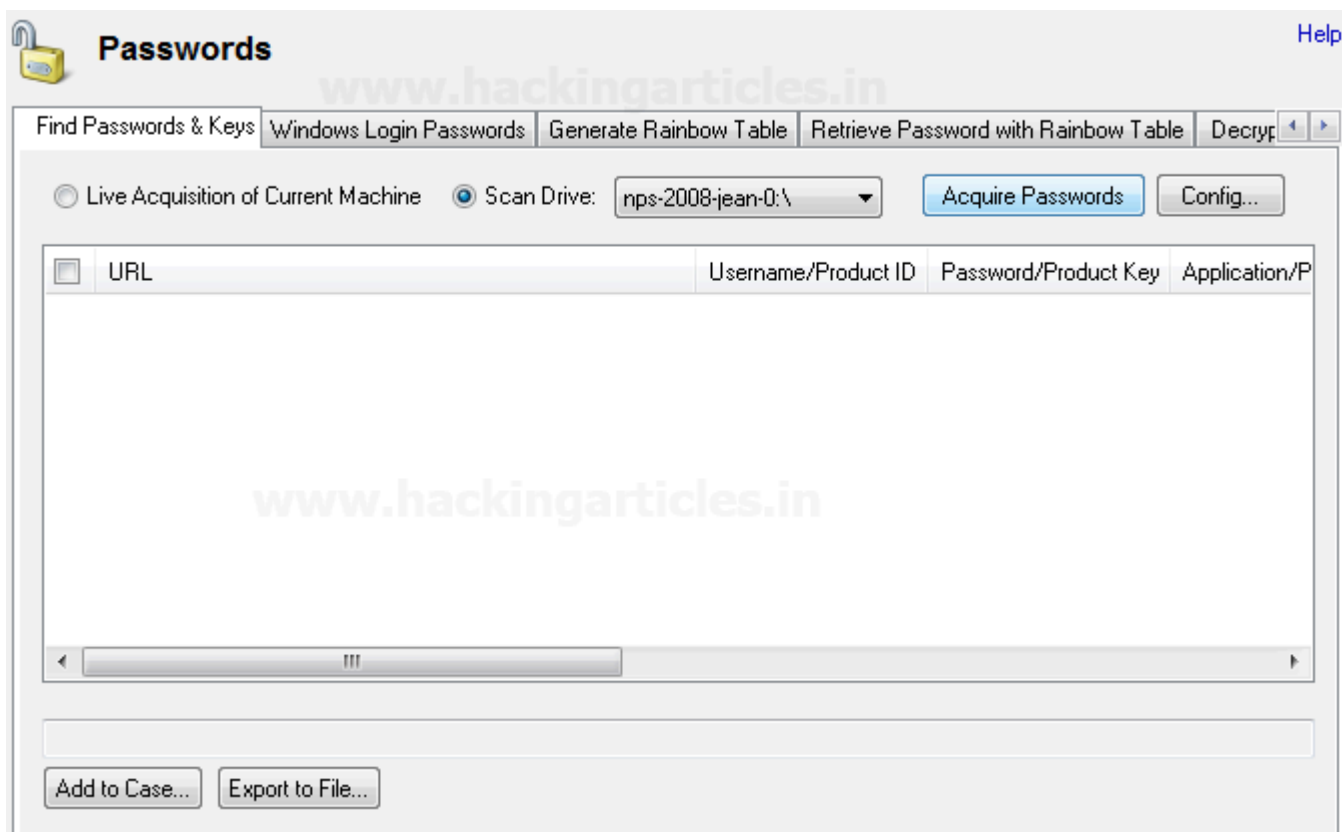


The first tab is to Find Passwords & Keys, this will allow recovering the stored password from the browser, outlook, windows auto logon passwords, etc. We can either do the live acquisition of current machine or Scan Drive and select any drive or evidence.

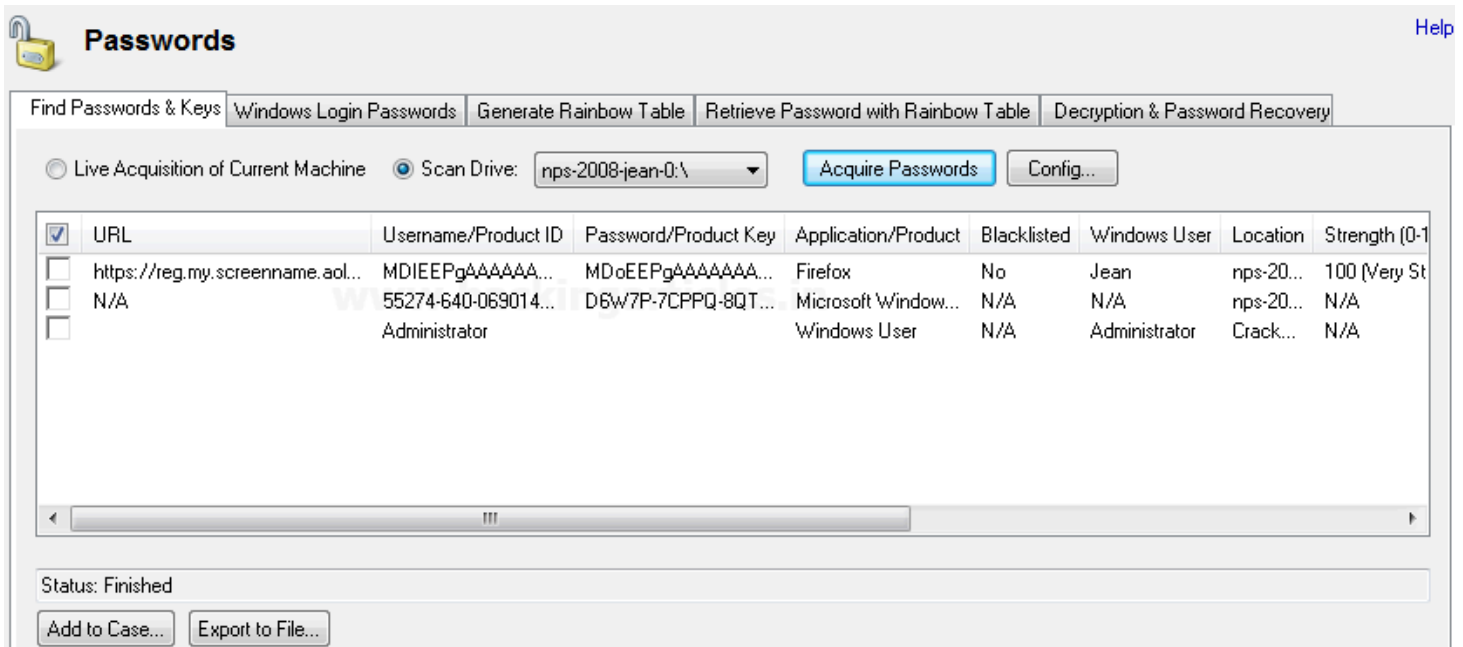
Click on the Config button, check the passwords you want to recover. Select the decryption settings based on requirements, we can include our dictionary file or can use an automatic dictionary. If credentials are known we can provide windows login credentials and click OK.



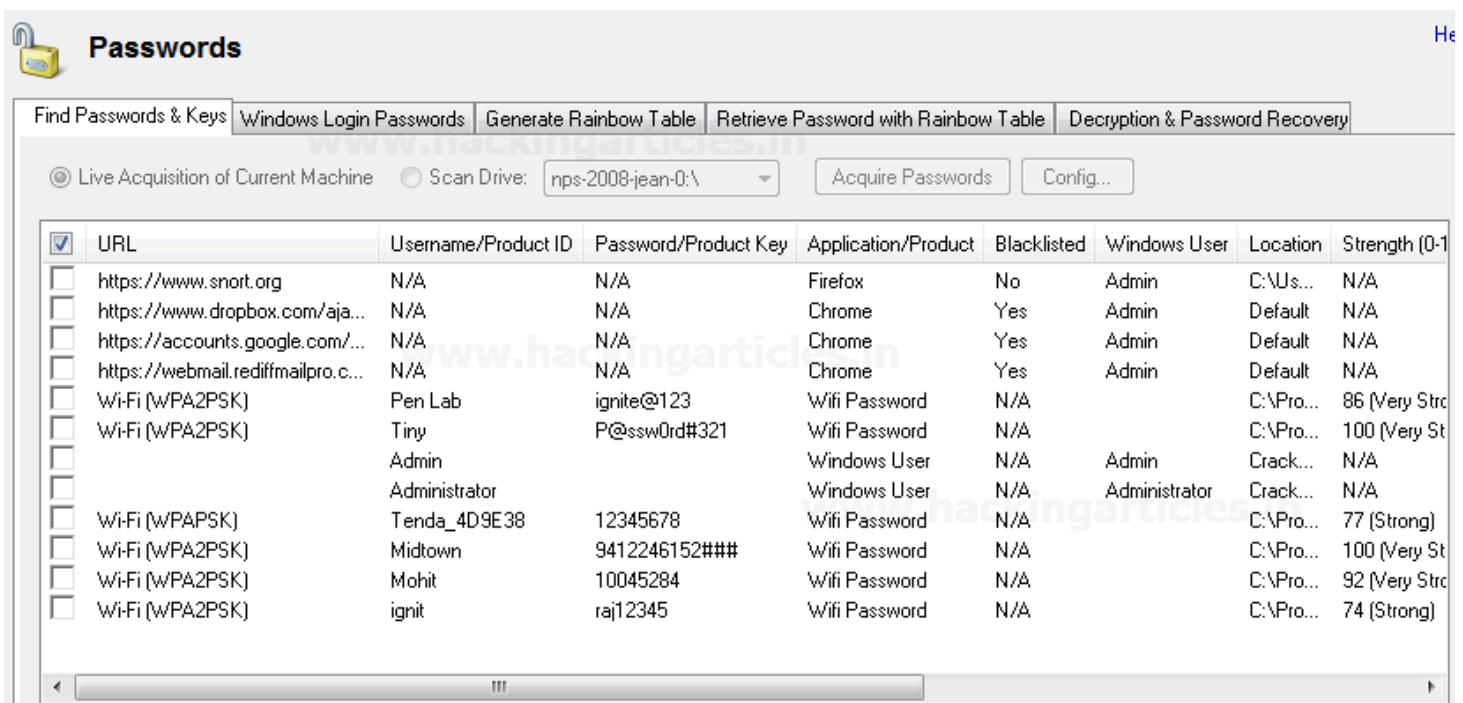
Click on Acquire passwords button to start the process.



All the passwords/product keys will get listed.

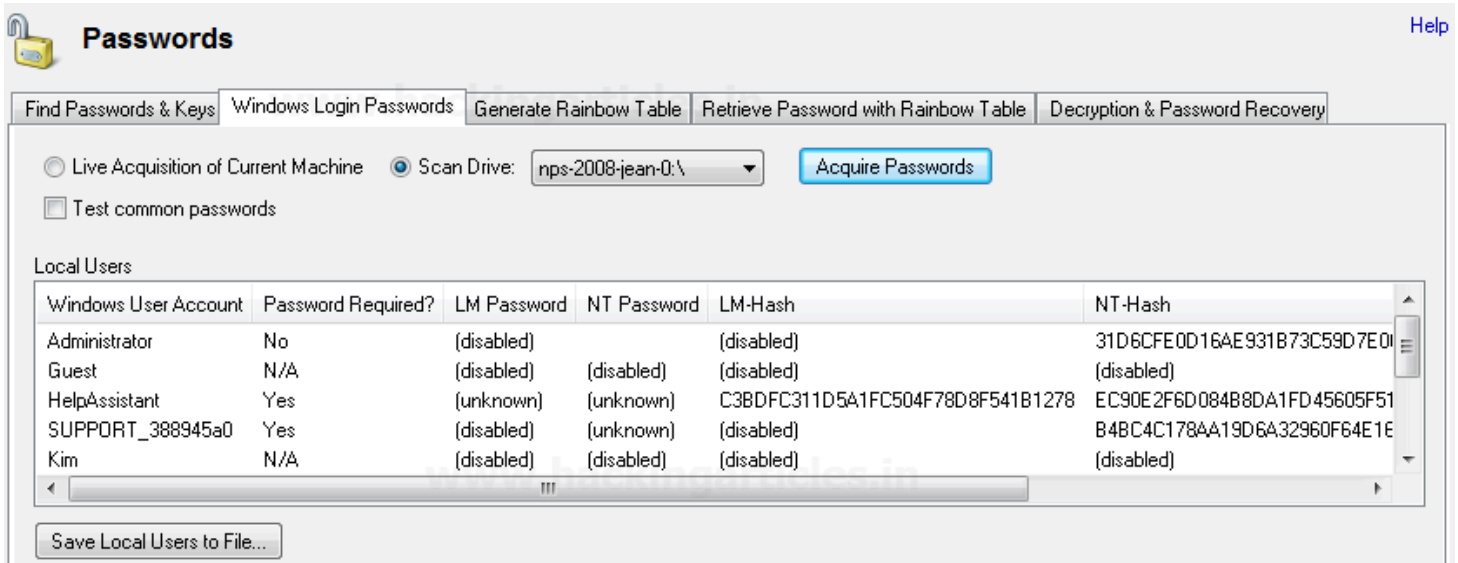


The below image is the passwords acquisition of the Current Machine for better understanding as the evidence we were working on doesn't have any stored wireless network.

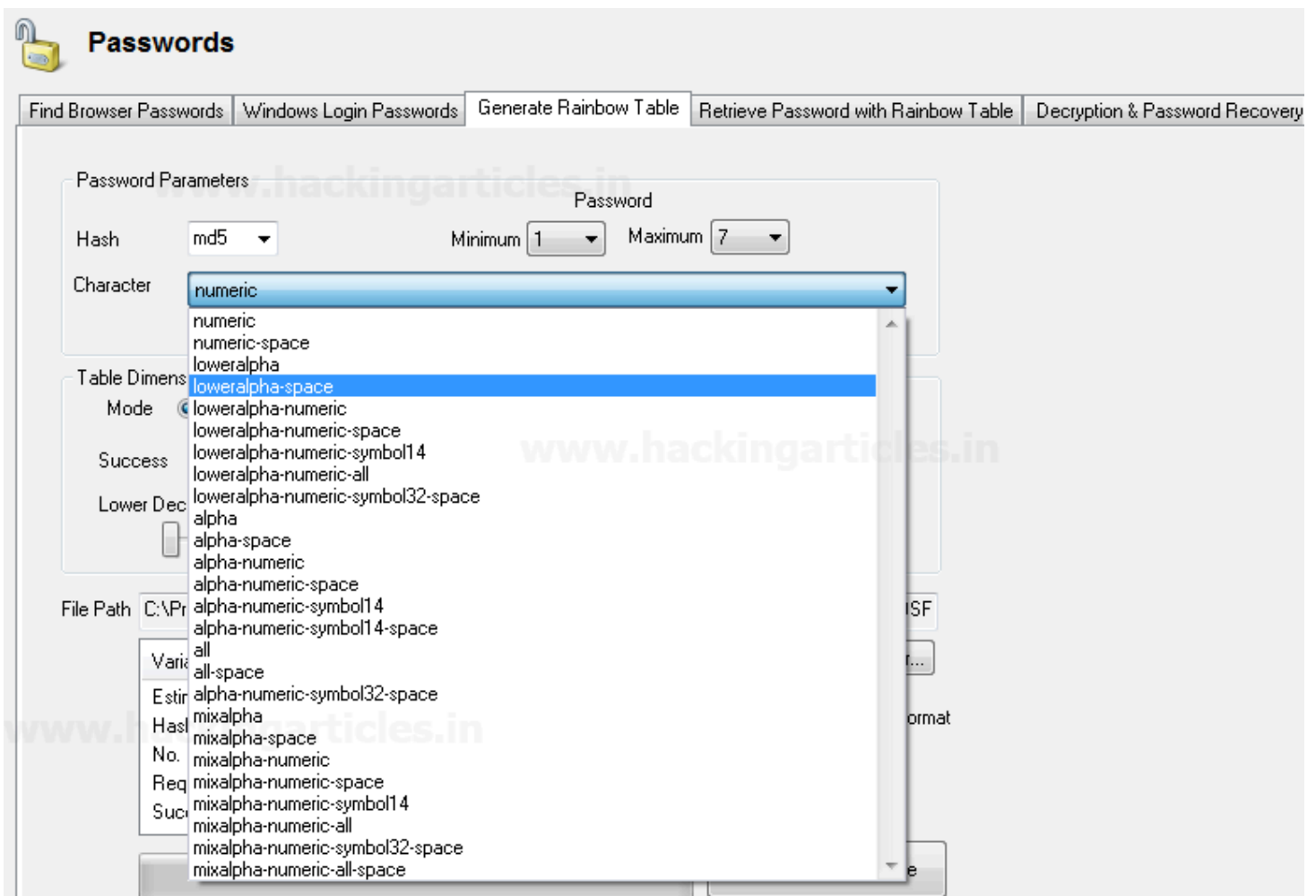


Select Windows Login Password , select the Drive/evidence and click Acquire passwords

All the information will get listed. If there is any saved password it will get listed also we can get info about it also we can get NT hash and LM Hash of the password from which we can recover the password.



We have an option to generate a rainbow table. This is used to create a list of passwords with different combinations and permutations. We can choose from the different options/combinations from the drop down. More huge and complex the inputs are the longer the time it will take.



Browse the file path where we want to save the table and if required modify the parameters. Click on create a rainbow table button to start with the process.

Depending on the complexity the process will start.

Passwords

Find Browser Passwords | Windows Login Passwords | **Generate Rainbow Table** | Retrieve Password with Rainbow Table

Password Parameters

Hash: md5 | Minimum: 1 | Maximum: 7 | Character: numeric | 0123456789

Table Dimensions

Mode: ☒ Automatic | ☐ Manual (Advanced Users)

Success: 95 % | Chain Length: 392 | Chain Count: 195608

Lower Decrypt: [Slider] | Lower File: [Slider]

File Path: C:\ProgramData\PassMark\OSForensics\RainbowTables\md5_numeric#1-7_0_392x195608_OSF

Variable	Value
Estimated Time to complete	< 1 minute
Hashes Per Second	7128292
No. of possible passwords	11111110
Required Disk Space	2.98 MB
Success Rate	95.06%

Save to Folder... | ☒ Compress to RTC format

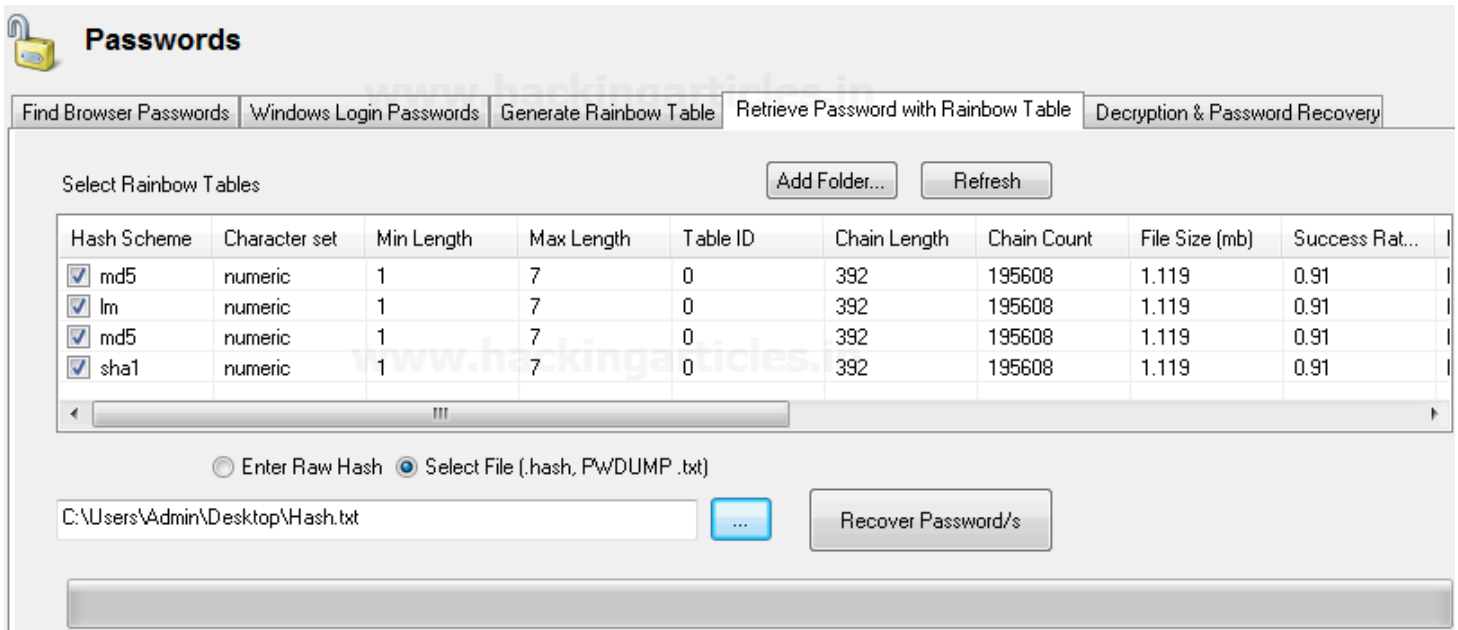
Cancel

Stage 1 of 3

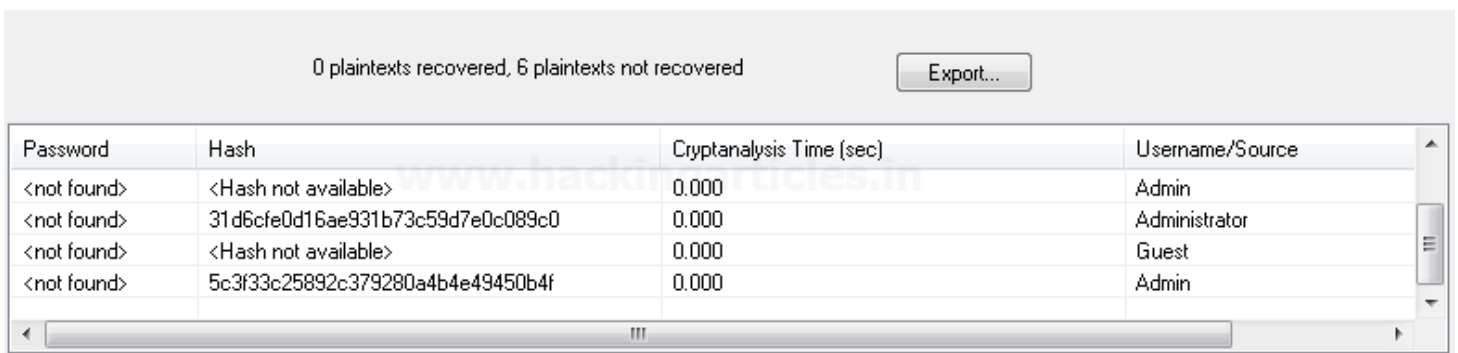
Generating Rainbow Table Segments

Password through a rainbow table. If the password is within the rainbow table we have created and we have the NT hash and LM Hash we can recover the passwords (however this). TO achieve this we need to add the folder of the Rainbow table under “Select Rainbow Table” and can either enter the raw hash or can browse the file which may contain the hash, if the password is present within the rainbow table, we will get the password.

In the image we are browsing the file “hash.txt”, we have saved in windows login password (shown above)and the rainbow table we have created.



Click on recover Password/s button to start the process, if the password present in Hash.txt is found in the rainbow table we will get the result.



In the above, we haven't found the password as it must be not present inside the table. Also, these tables have certain limitations and have a success rate of 95 % (approx). There are other methods as well for the recovery of passwords we will be discussing on other articles.

This concludes Passwords.

For more on OSForensics wait for the next article.