Digital Forensics Investigation through OS Forensics (Part 2)

January 30, 2018 By Raj Chandel

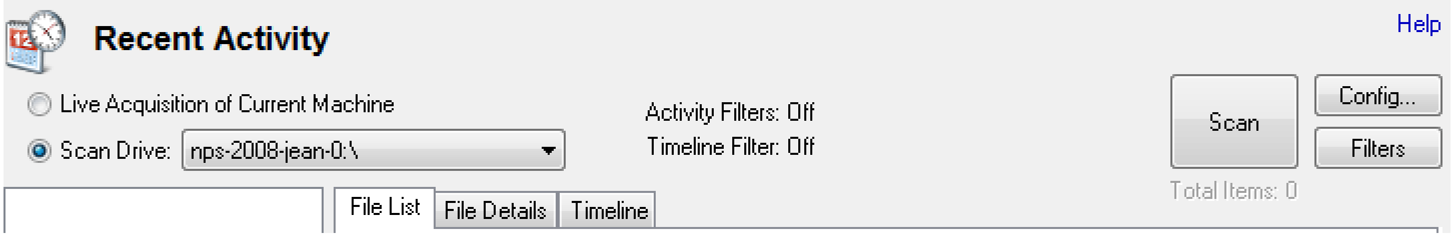
In Part 1 of this article, we have covered Creating case, File Search and Indexing. This article will cover some more features/ functionalities of OSForensics.

For Part 1 if this article clicks **here**.

Recent Activity

Recent Activity feature allows an investigator to scan the evidence for recent activity, such as accessed websites, USB drives, wireless networks, recent downloads and many more.

To start with open OSForensics and select Recent Activity.



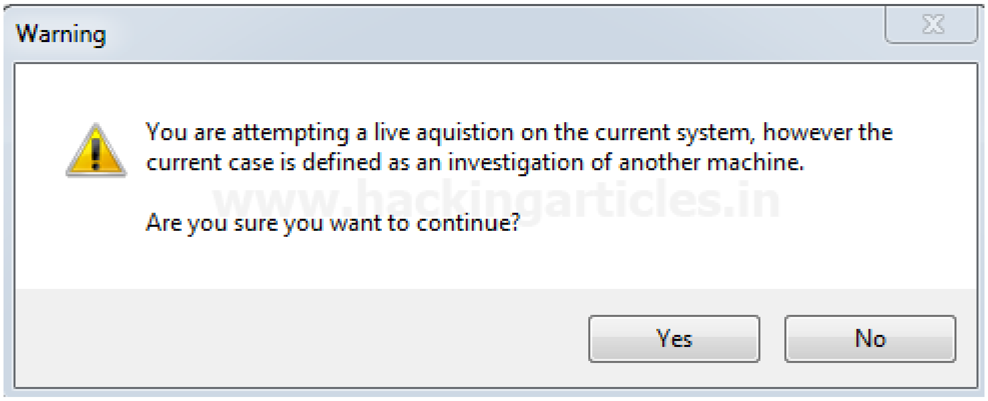
○ Live Acquisition of Current Machine
● Scan Drive: nps-2008-jean-0:\

Activity Filters: Off
Timeline Filter: Off

Total Items: 0

We have an option to capture the Recent Activities either through the live acquisition of current machines or by scanning drives/evidence.

To capture the live acquisition of the current machine select the first option and click on scan. If we have opted to investigate the case of another machine at the time of creating the case (shown in part 1 of this article), we may get a warning message as shown below, Click on yes to continue.



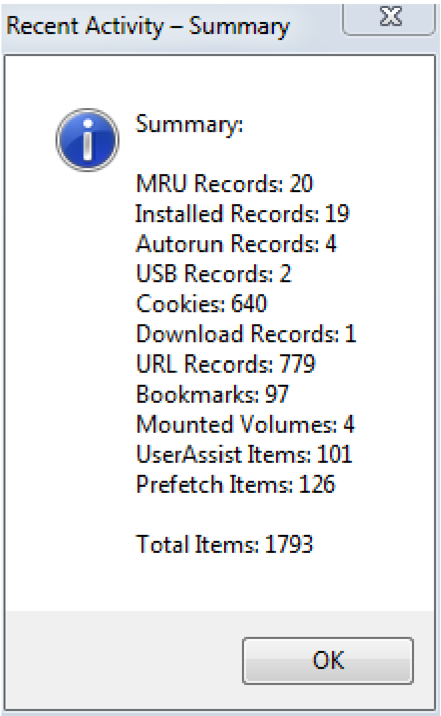
You are attempting a live aquistion on the current system, however the current case is defined as an investigation of another machine.

Are you sure you want to continue?

But we will be acquiring our evidence (.E01 image file).

Scanning will start and may take some time for this operation to complete.

Once the scanning is complete we will get a pop up with the summary of the scanned evidence.



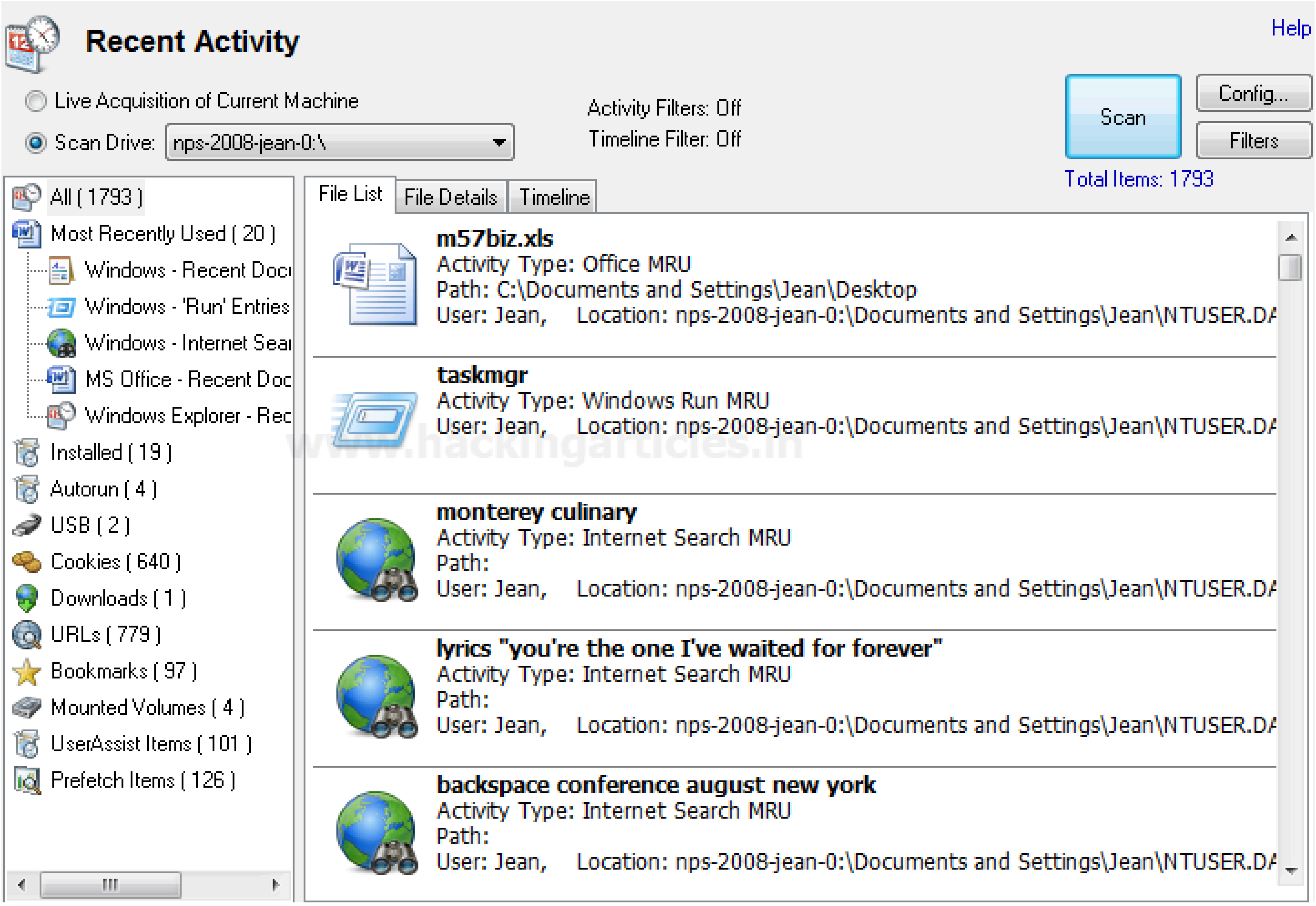
Summary:

MRU Records: 20
Installed Records: 19
Autorun Records: 4
USB Records: 2
Cookies: 640
Download Records: 1
URL Records: 779
Bookmarks: 97
Mounted Volumes: 4
UserAssist Items: 101
Prefetch Items: 126

Total Items: 1793

Click on the OK button and on the recent activity window we can find all the recent activity details with the heading on the left pane and details of related files on the right.

Below is the list view of the files



○ Live Acquisition of Current Machine
● Scan Drive: nps-2008-jean-0:\

Activity Filters: Off
Timeline Filter: Off

Total Items: 1793

All (1793)
Most Recently Used (20)
Windows - Recent Docı
Windows - 'Run' Entries
Windows - Internet Sear
MS Office - Recent Doc
Windows Explorer - Rec
Installed (19)
Autorun (4)
USB (2)
Cookies (640)
Downloads (1)
URLs (779)
Bookmarks (97)
Mounted Volumes (4)
UserAssist Items (101)
Prefetch Items (126)

m57biz.xls
Activity Type: Office MRU
Path: C:\Documents and Settings\Jean\Desktop
User: Jean, Location: nps-2008-jean-0:\Documents and Settings\Jean\NTUSER.DA

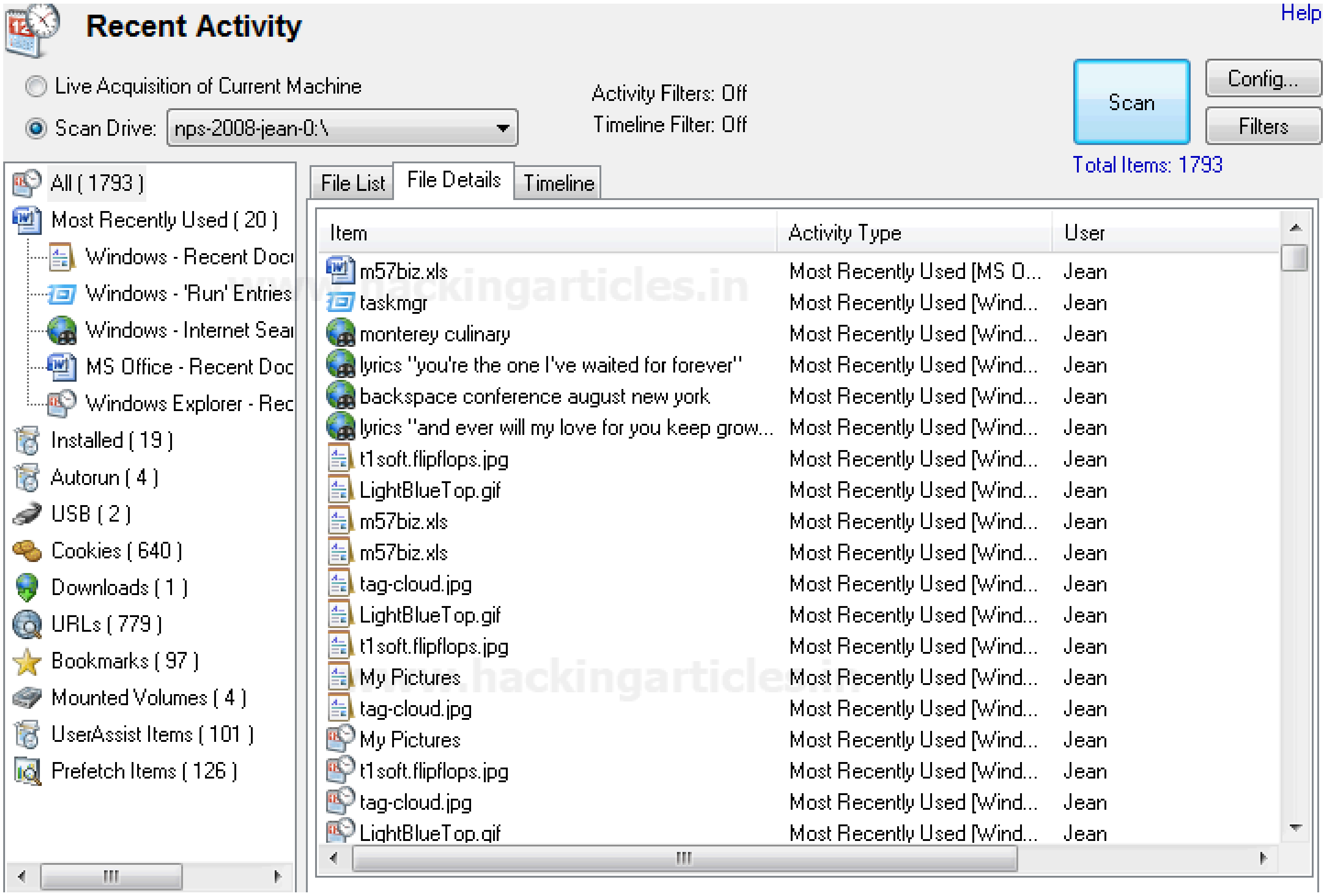
taskmgr
Activity Type: Windows Run MRU
User: Jean, Location: nps-2008-jean-0:\Documents and Settings\Jean\NTUSER.DA

monterey culinary
Activity Type: Internet Search MRU
Path:
User: Jean, Location: nps-2008-jean-0:\Documents and Settings\Jean\NTUSER.DA

lyrics "you're the one I've waited for forever"
Activity Type: Internet Search MRU
Path:
User: Jean, Location: nps-2008-jean-0:\Documents and Settings\Jean\NTUSER.DA

backspace conference august new york
Activity Type: Internet Search MRU
Path:
User: Jean, Location: nps-2008-jean-0:\Documents and Settings\Jean\NTUSER.DA

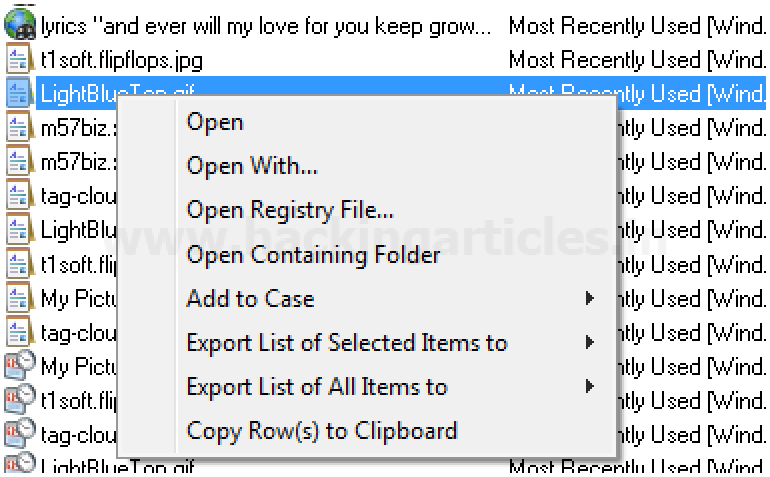
We can also view the file details by clicking on the File Details tab



Activity Filters: Off
Timeline Filter: Off

Item	Activity Type	User
m57biz.xls	Most Recently Used [MS O...	Jean
taskmgr	Most Recently Used [Wind...	Jean
monterey culinary	Most Recently Used [Wind...	Jean
lyrics "you're the one I've waited for forever"	Most Recently Used [Wind...	Jean
backspace conference august new york	Most Recently Used [Wind...	Jean
lyrics "and ever will my love for you keep grow...	Most Recently Used [Wind...	Jean
t1soft.flipflops.jpg	Most Recently Used [Wind...	Jean
LightBlueTop.gif	Most Recently Used [Wind...	Jean
m57biz.xls	Most Recently Used [Wind...	Jean
m57biz.xls	Most Recently Used [Wind...	Jean
tag-cloud.jpg	Most Recently Used [Wind...	Jean
LightBlueTop.gif	Most Recently Used [Wind...	Jean
t1soft.flipflops.jpg	Most Recently Used [Wind...	Jean
My Pictures	Most Recently Used [Wind...	Jean
tag-cloud.jpg	Most Recently Used [Wind...	Jean
My Pictures	Most Recently Used [Wind...	Jean
t1soft.flipflops.jpg	Most Recently Used [Wind...	Jean
tag-cloud.jpg	Most Recently Used [Wind...	Jean
LightBlueTop.gif	Most Recently Used [Wind...	Jean

To further analyze any file, simply right-click on file for further file options.

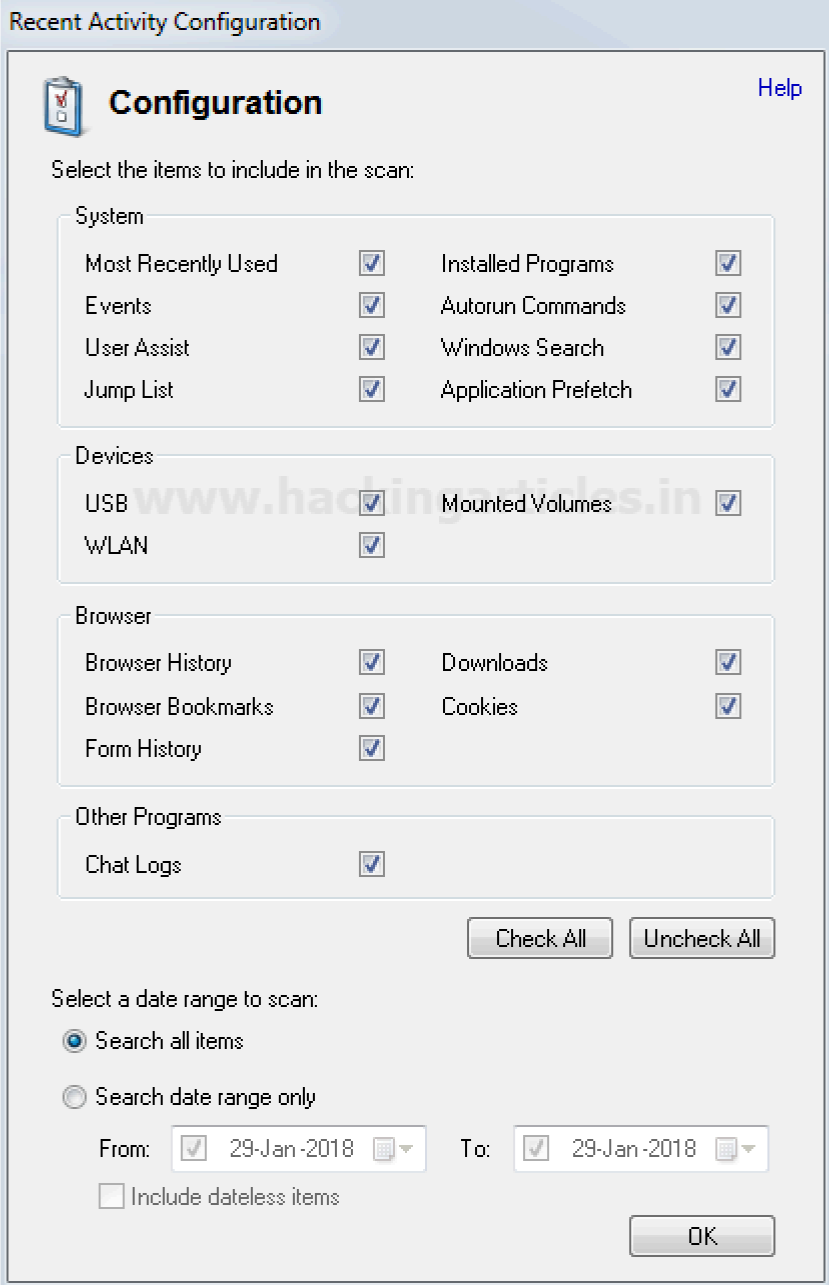


lyrics "and ever will my love for you keep grow... Most Recently Used [Wind.
t1soft.flipflops.jpg Most Recently Used [Wind.
LightBlueTop.gif Most Recently Used [Wind.

Similarly, we can investigate the recent activity of any particular drive.

We can also change the configurations or apply/remove any filters as per the requirement but these changes are to be done before starting the scan.

To edit the configurations click on “Config” button located at the top right corner on recent activity window.



Recent Activity Configuration

Configuration

Select the items to include in the scan:

System

Most Recently Used ☑ Installed Programs ☑
Events ☑ Autorun Commands ☑
User Assist ☑ Windows Search ☑
Jump List ☑ Application Prefetch ☑

Devices

USB ☑ Mounted Volumes ☑
WLAN ☑

Browser

Browser History ☑ Downloads ☑
Browser Bookmarks ☑ Cookies ☑
Form History ☑

Other Programs

Chat Logs ☑

Select a date range to scan:

● Search all items

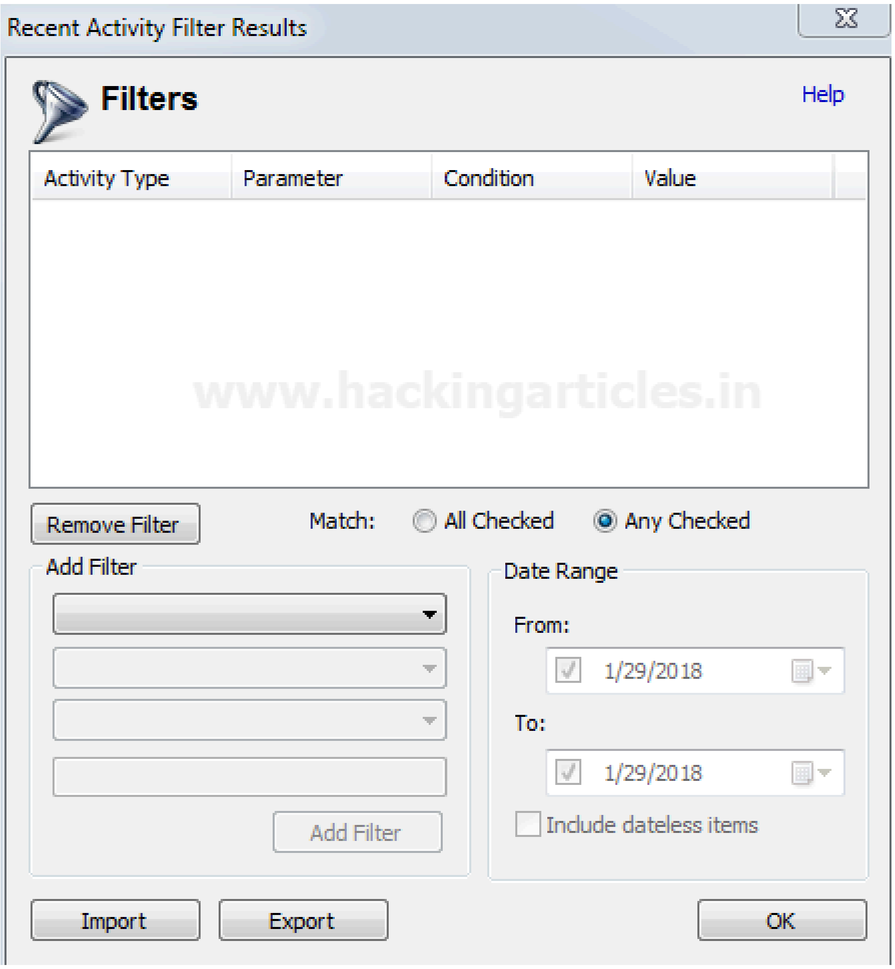
○ Search date range only

From: ☑ 29-Jan -2018 To: ☑ 29-Jan -2018

□ Include dateless items

Check/Uncheck the options as required or if required change the date/date range for a particular time-based activity and click OK.

For managing the filters click on the “Filters” button located below the “Config” button



Recent Activity Filter Results

Filters

Activity Type	Parameter	Condition	Value

Match: ○ All Checked ● Any Checked

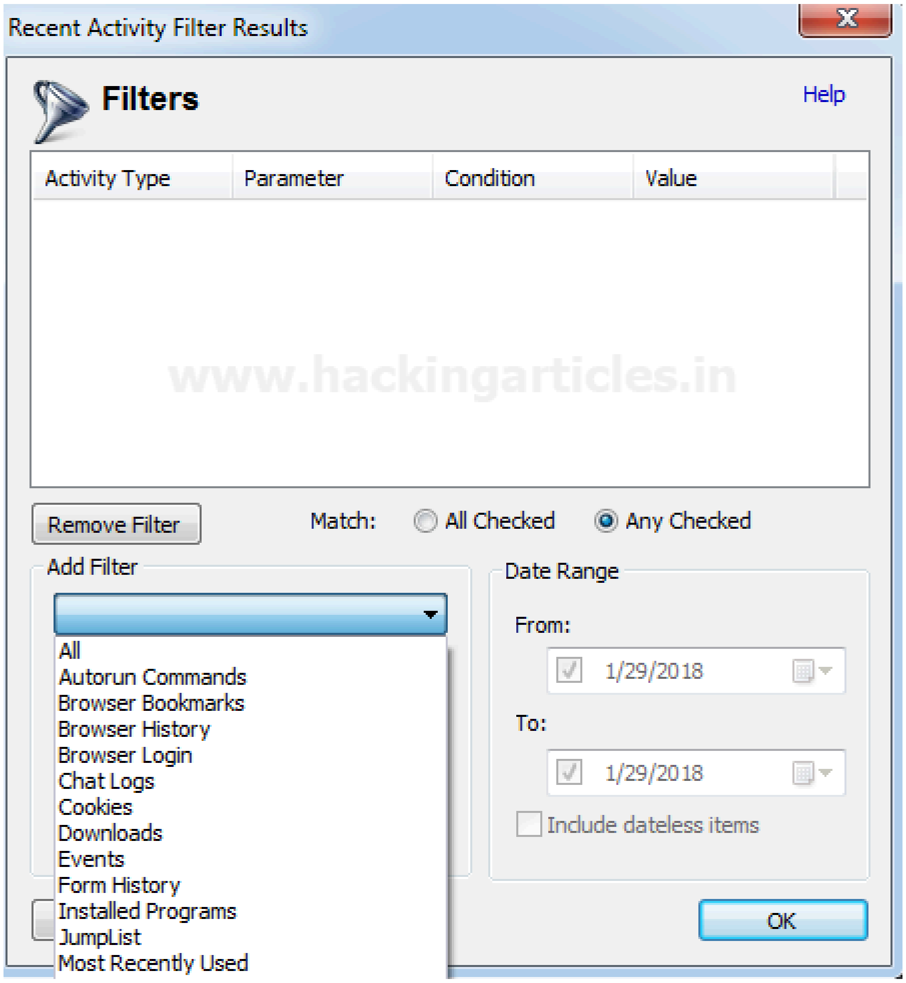
Date Range

From: ☑ 1/29/2018

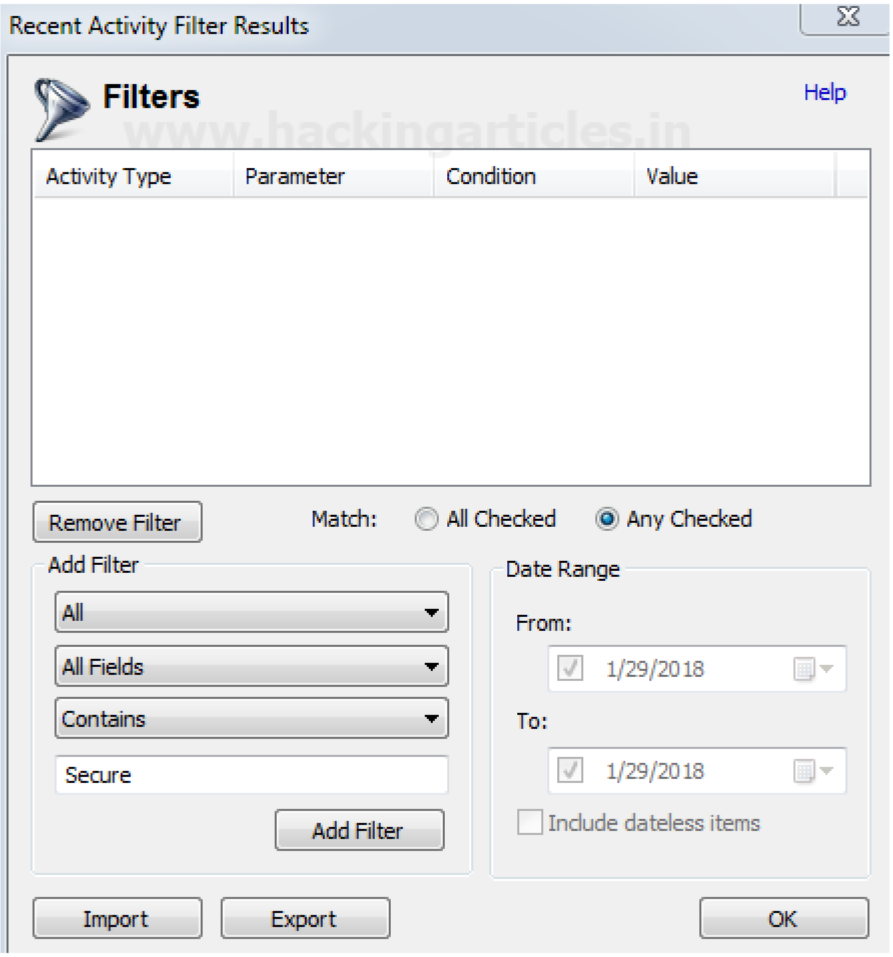
To: ☑ 1/29/2018

□ Include dateless items

We can add a filter as required by selecting a value from the drop-down or fill the details as required.



In the below image we have applied a filter and set its parameters as per requirement.



Activity Type	Parameter	Condition	Value

Match: ○ All Checked ● Any Checked

Add Filter

All

All Fields

Contains

Secure

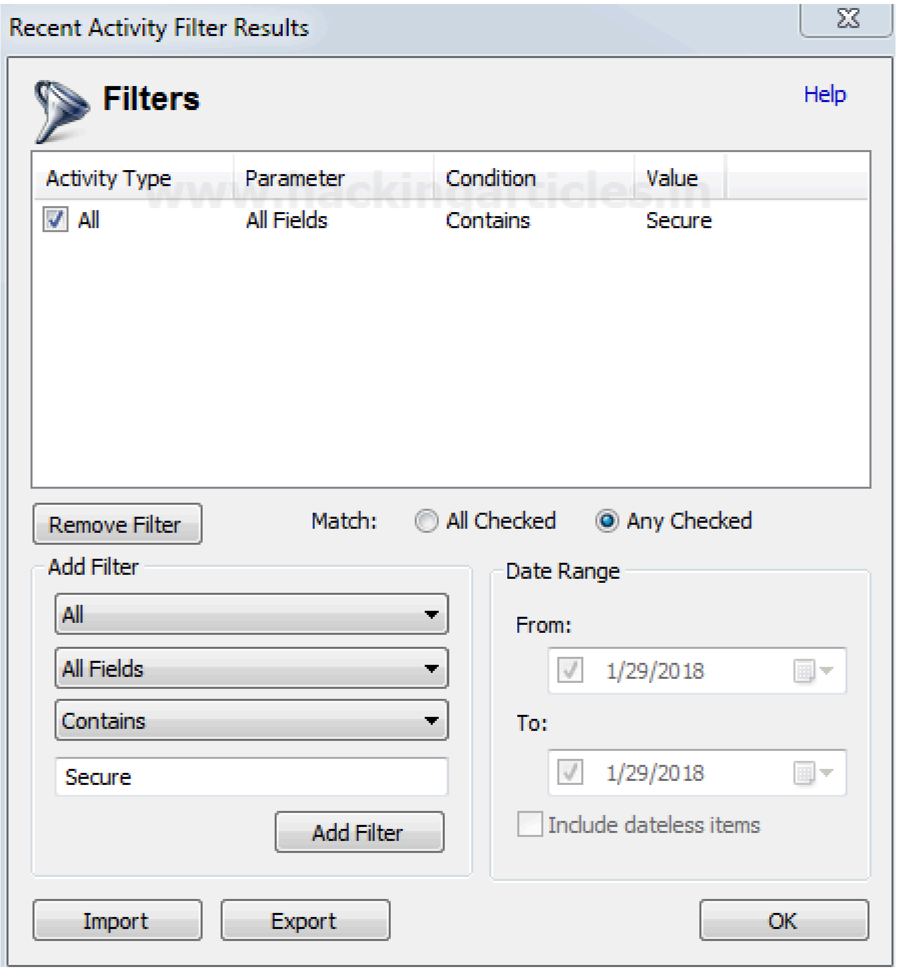
Date Range

From: ☑ 1/29/2018

To: ☑ 1/29/2018

□ Include dateless items

Click on Add Filter button and then OK, the filter will get added.



Recent Activity Filter Results

Filters

Activity Type	Parameter	Condition	Value
☑ All	All Fields	Contains	Secure

Match: ○ All Checked ● Any Checked

Add Filter

- All
- All Fields
- Contains
- Secure

Date Range

From: ☑ 1/29/2018

To: ☑ 1/29/2018

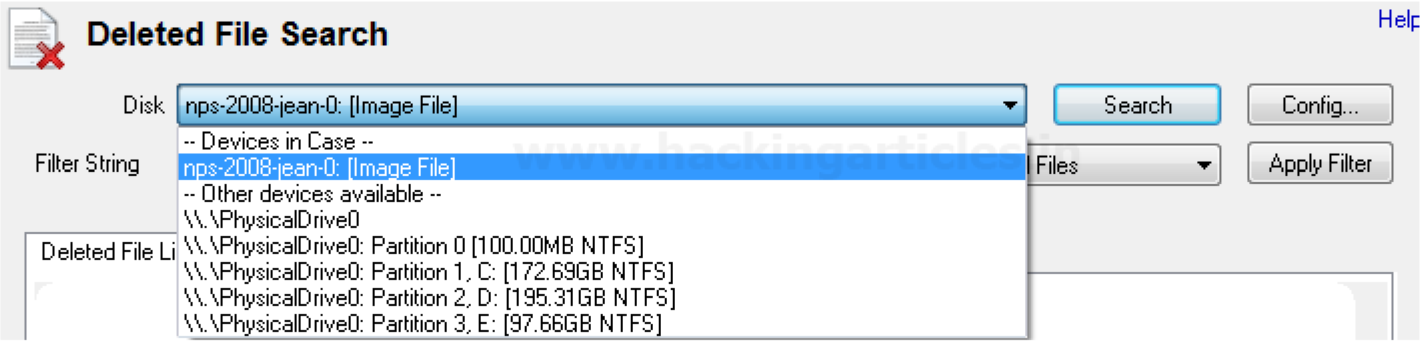
□ Include dateless items

This ends the Recent Activity feature.

Deleted File Search

Deleted files recovery is one of the prime requirements for digital forensics. OSF offers a very simple and efficient deleted file recovery/search.

To search the deleted files click on "Deleted files Search" and select the drive we want to search on from the drop-down. We can select the complete Physical drive/Hard Disk (PhysicalDrive0), Acquired Evidence or any Logical drive(C/D/E), for which we want to recover the data.



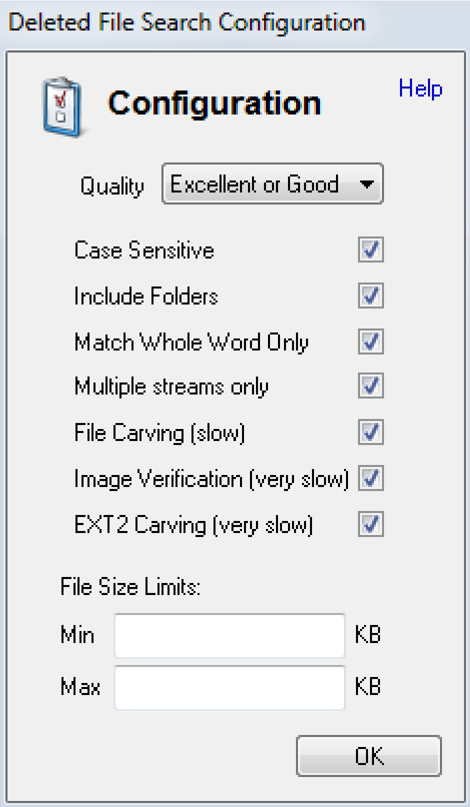
Deleted File Search

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

```
-- Devices in Case --
nps-2008-jean-0: [Image File]
-- Other devices available --
\\.\PhysicalDrive0
\\.\PhysicalDrive0: Partition 0 [100.00MB NTFS]
\\.\PhysicalDrive0: Partition 1, C: [172.69GB NTFS]
\\.\PhysicalDrive0: Partition 2, D: [195.31GB NTFS]
\\.\PhysicalDrive0: Partition 3, E: [97.66GB NTFS]
```

Click on the "Config" button and check/uncheck the options as required. Select the Quality from the drop-down (Please note better the quality more time it will take to process), for better result check the file carving option.

We can also limit the file size we want to search for (this will omit the files that are not in the range to refine the search), Click Ok.

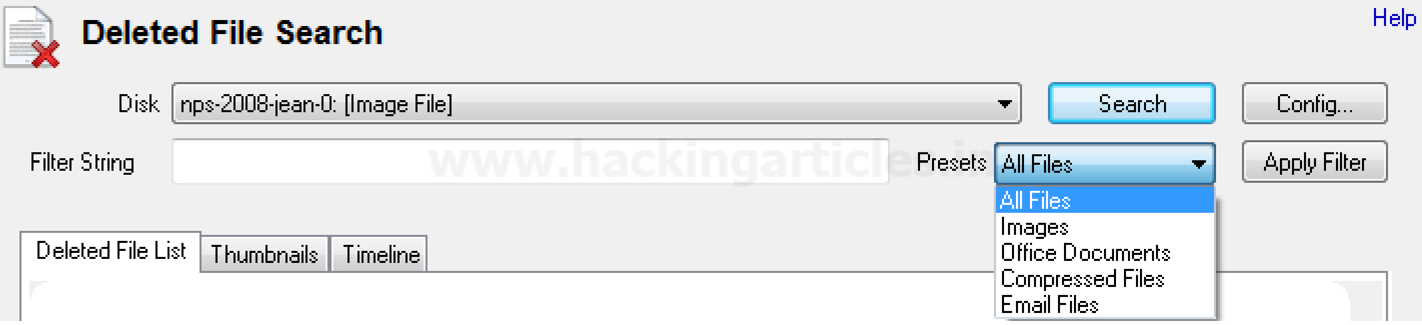


Quality: Excellent or Good

☑ Case Sensitive
☑ Include Folders
☑ Match Whole Word Only
☑ Multiple streams only
☑ File Carving (slow)
☑ Image Verification (very slow)
☑ EXT2 Carving (very slow)

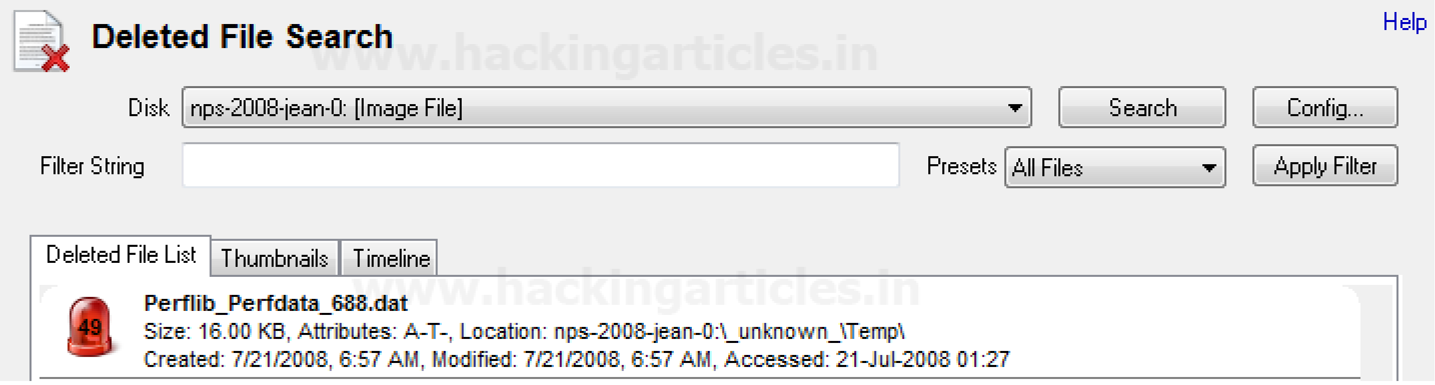
File Size Limits:
Min ____ KB
Max ____ KB

On preset drop-down select the file type we want to recover/search. Select all files if we need to have multiple file types as output.



Disk: nps-2008-jean-0: [Image File]
Filter String:
Presets: All Files

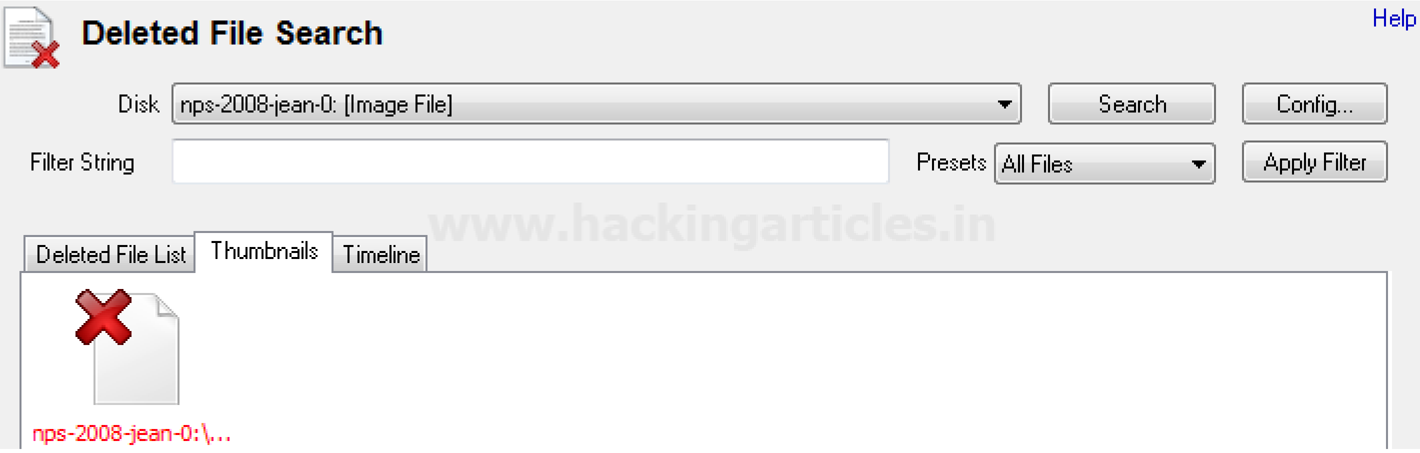
Once all the settings are done, click on Search. Depending on the volume of data and configurations we opted for it may take some time for the process to complete.



Disk: nps-2008-jean-0: [Image File]
Filter String:
Presets: All Files

Perflib_Perfdata_688.dat
Size: 16.00 KB, Attributes: A-T-, Location: nps-2008-jean-0:_unknown_\Temp\
Created: 7/21/2008, 6:57 AM, Modified: 7/21/2008, 6:57 AM, Accessed: 21-Jul-2008 01:27

We can also see the thumbnail view of the files for faster analysis.



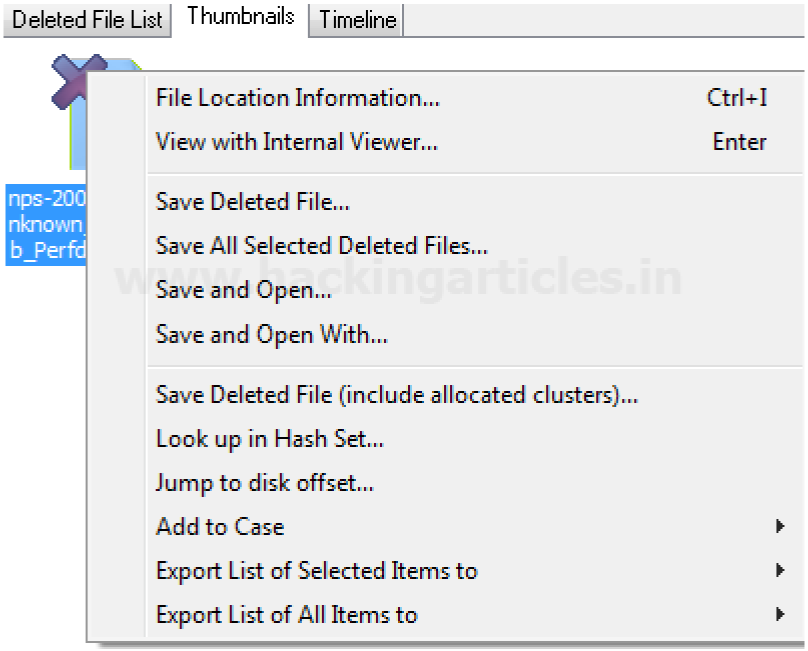
Deleted File Search

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

Filter String:

Presets: All Files

To save /recover the file select the files we want to recover and right-click for options and save the files.



Deleted File List
Thumbnails
Timeline
nps-200
nknown
b_Perfd
File Location Information... Ctrl+I
View with Internal Viewer... Enter
Save Deleted File...
Save All Selected Deleted Files...
Save and Open...
Save and Open With...
Save Deleted File (include allocated clusters)...
Look up in Hash Set...
Jump to disk offset...
Add to Case
Export List of Selected Items to
Export List of All Items to

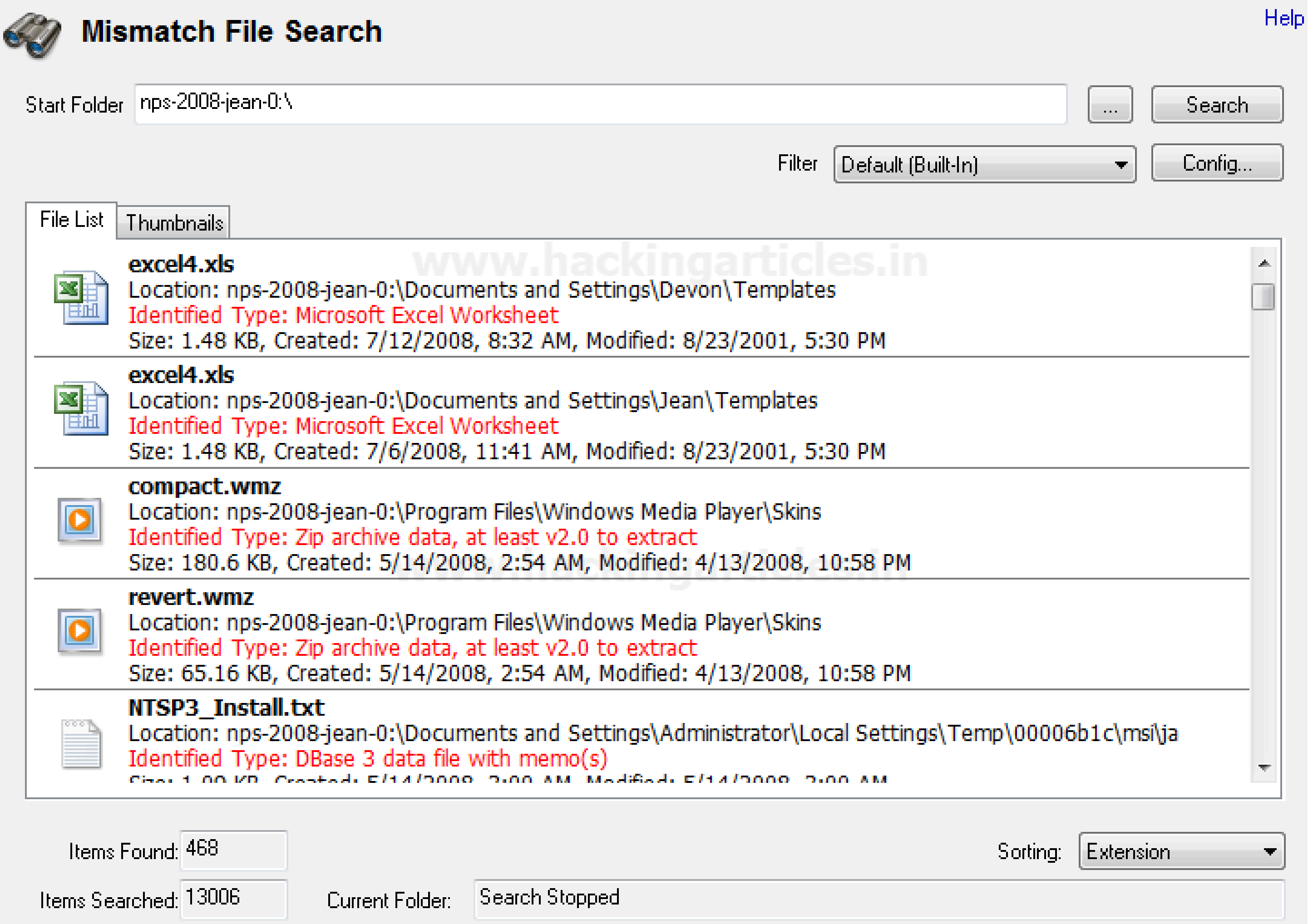
This concludes the Deleted file search.

Mismatch File Search

This feature enables us to identify the files whose extensions don’t match their data. Through this, we can capture some relevant evidence that could be in form of an image, document or pdf but pretending to be of some other extension. For example, a word file can be mismatched with a jpeg file (such a data could be also called “Dark Data”).

To start with click on Mismatch File Search, select the drive/directory along with the filter from the drop-down or create a filter as required, if we are not sure about the filter settings, we can go with “All (Built In)” filter and click search.

This will show the result in the file list. We can also see the thumbnail view of the files.



Start Folder: nps-2008-jean-0:\

Filter: Default (Built-In)

excel4.xls
Location: nps-2008-jean-0:\Documents and Settings\Devon\Templates
Identified Type: Microsoft Excel Worksheet
Size: 1.48 KB, Created: 7/12/2008, 8:32 AM, Modified: 8/23/2001, 5:30 PM

excel4.xls
Location: nps-2008-jean-0:\Documents and Settings\Jean\Templates
Identified Type: Microsoft Excel Worksheet
Size: 1.48 KB, Created: 7/6/2008, 11:41 AM, Modified: 8/23/2001, 5:30 PM

compact.wmz
Location: nps-2008-jean-0:\Program Files\Windows Media Player\Skins
Identified Type: Zip archive data, at least v2.0 to extract
Size: 180.6 KB, Created: 5/14/2008, 2:54 AM, Modified: 4/13/2008, 10:58 PM

revert.wmz
Location: nps-2008-jean-0:\Program Files\Windows Media Player\Skins
Identified Type: Zip archive data, at least v2.0 to extract
Size: 65.16 KB, Created: 5/14/2008, 2:54 AM, Modified: 4/13/2008, 10:58 PM

NTSP3_Install.txt
Location: nps-2008-jean-0:\Documents and Settings\Administrator\Local Settings\Temp\00006b1c\msi\ja
Identified Type: DBase 3 data file with memo(s)
Size: 1.00 KB, Created: 5/14/2008, 2:00 AM, Modified: 5/14/2008, 2:00 AM

Items Found: 468

Sorting: Extension

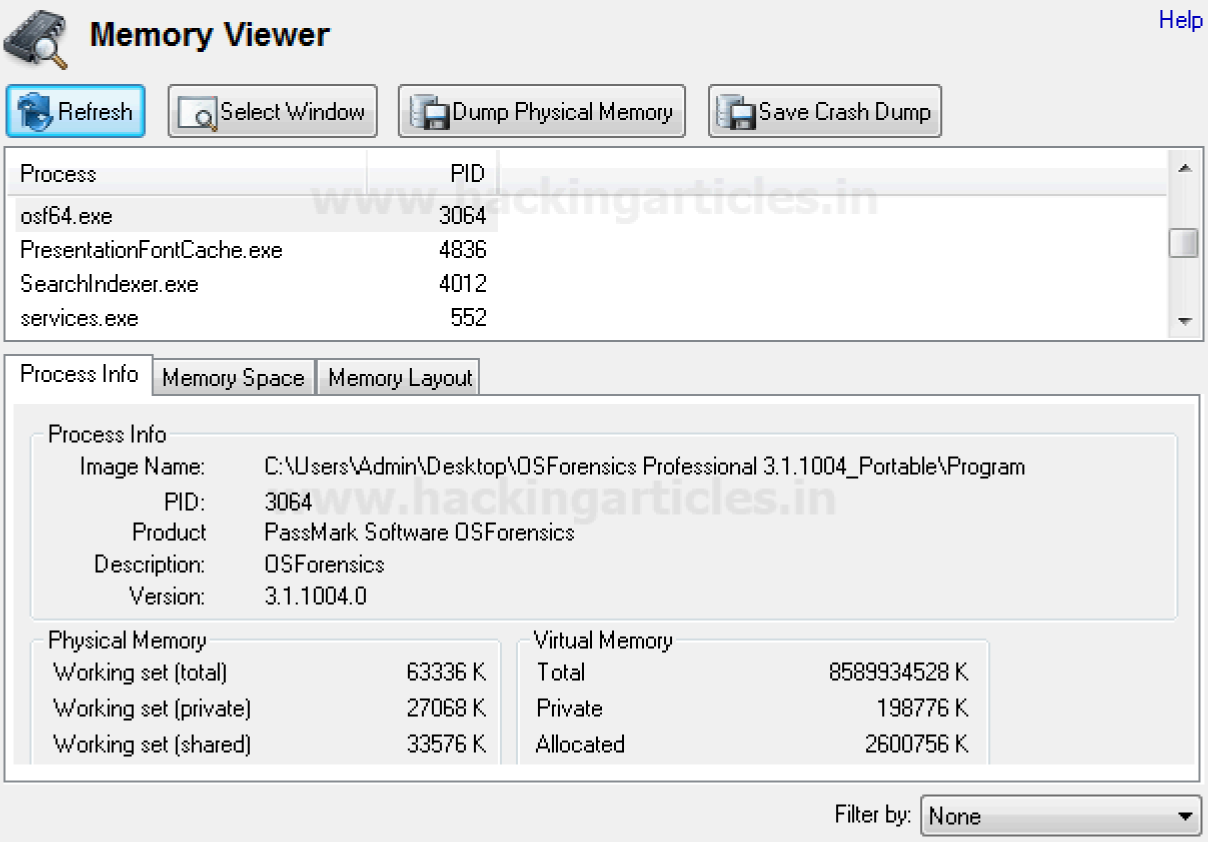
Items Searched: 13006

Current Folder: Search Stopped

Memory Viewer

Memory Viewer feature shows active memory of the system on which OSF is working on. It can’t be used to show the memory of acquired image or drive of another computer (we will illustrate this feature on our running machine and not on our evidence file). We can dump the live memory /RAM for further investigation.

To start with open OSF and click on Memory Viewer. We can see the list of all the processes currently running along with their Process ID (PID). Click on any process and we can see its details under process Info. Click on refresh to refresh the process list.



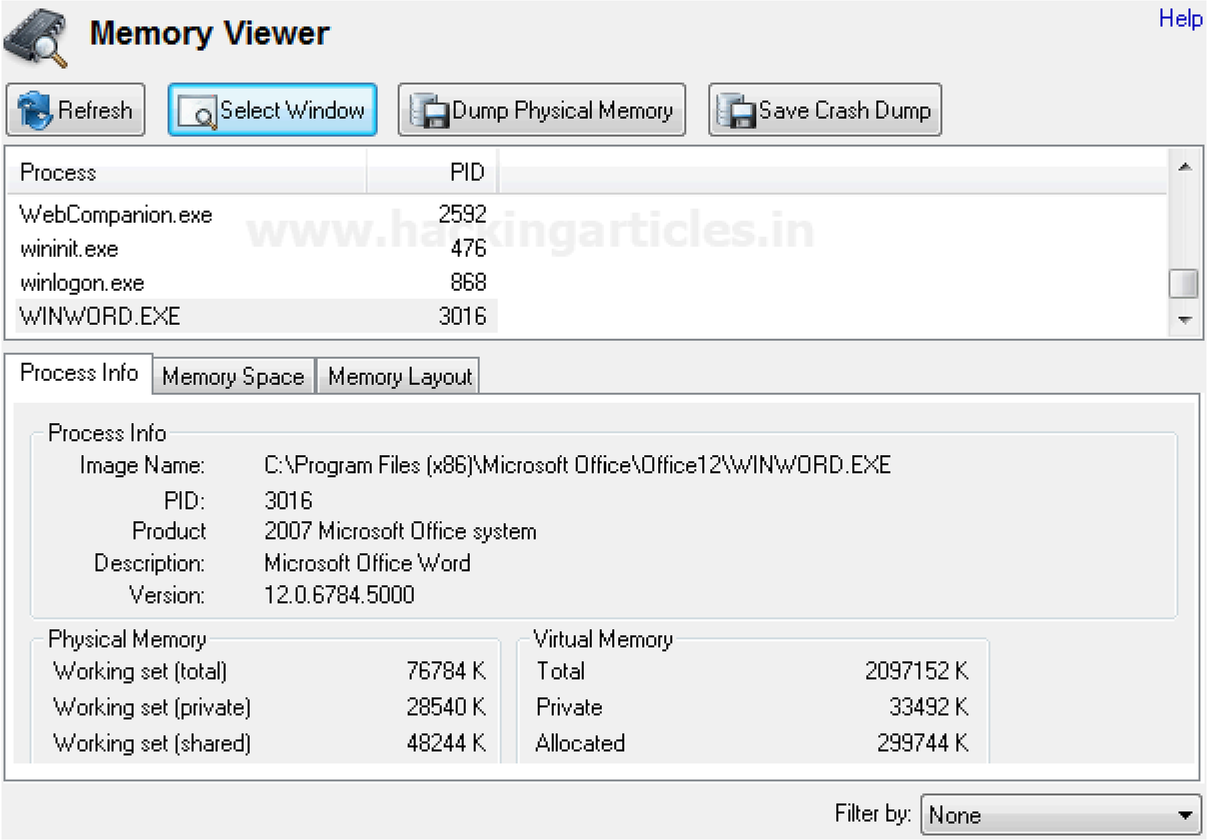
Process	PID
osf64.exe	3064
PresentationFontCache.exe	4836
SearchIndexer.exe	4012
services.exe	552

Process Info

Image Name: C:\Users\Admin\Desktop\OSForensics Professional 3.1.1004_Portable\Program
PID: 3064
Product PassMark Software OSForensics
Description: OSForensics
Version: 3.1.1004.0

Physical Memory		Virtual Memory	
Working set (total)	63336 K	Total	8589934528 K
Working set (private)	27068 K	Private	198776 K
Working set (shared)	33576 K	Allocated	2600756 K

Click on the select window the cursor icon will change from pointer to a circle, click anywhere on-screen or on any other running application and we can see the process details of the process we have clicked on. For instance, in the below image we have clicked on an open word file and the process corresponding to that word file will get displayed.



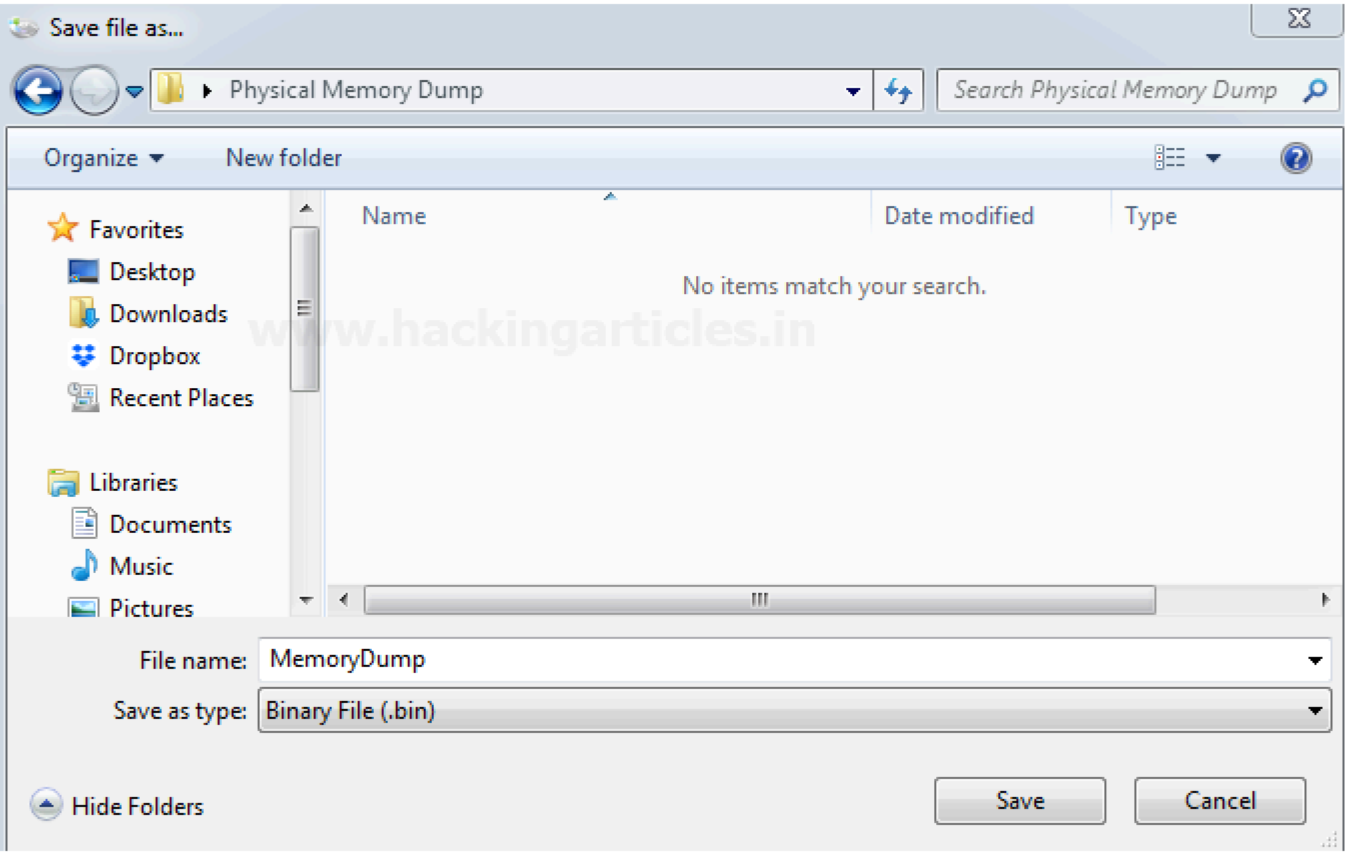
Process	PID
WebCompanion.exe	2592
wininit.exe	476
winlogon.exe	868
WINWORD.EXE	3016

Process Info

Image Name: C:\Program Files (x86)\Microsoft Office\Office12\WINWORD.EXE
PID: 3016
Product 2007 Microsoft Office system
Description: Microsoft Office Word
Version: 12.0.6784.5000

Physical Memory		Virtual Memory	
Working set (total)	76784 K	Total	2097152 K
Working set (private)	28540 K	Private	33492 K
Working set (shared)	48244 K	Allocated	299744 K

Click on dump Physical Memory, this will dump the physical memory/ RAM in a .bin file and can save it anywhere. In below image, we are saving the file with name Memory Dump.bin in a folder named Physical Memory Dump on Desktop

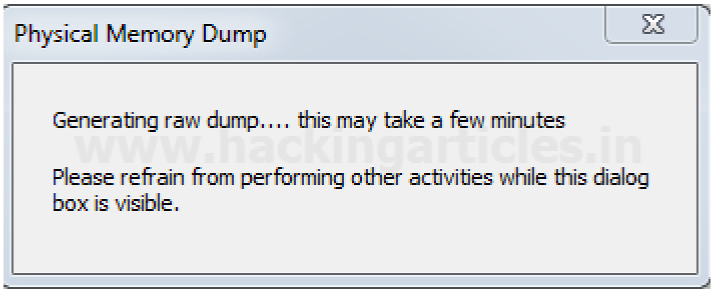


No items match your search.

File name: MemoryDump

Save as type: Binary File (.bin)

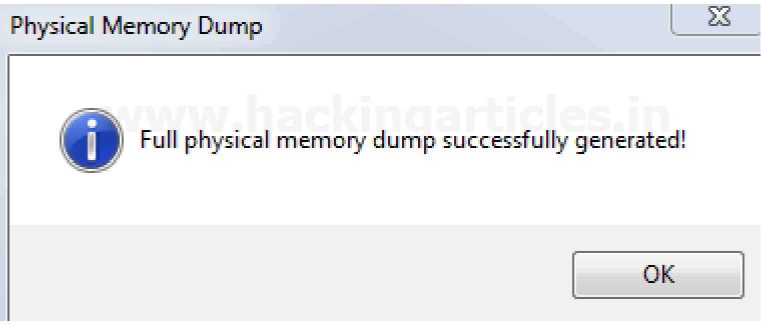
As we click on save pop up will appear till the Memory is being dumped.



Generating raw dump.... this may take a few minutes

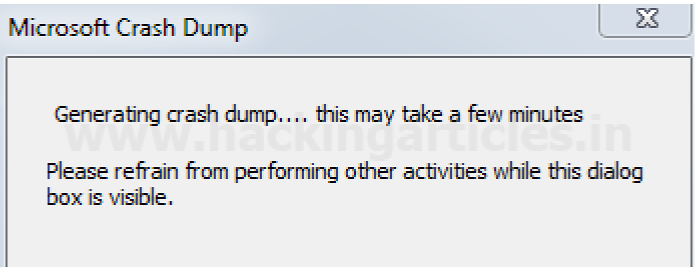
Please refrain from performing other activities while this dialog box is visible.

Once completed, we will get a success Message.



Full physical memory dump successfully generated!

We can also save a crash dump, just browse to a directory and save the file. The extension of the crash dump file is .dmp. In the below image, we are saving a crash dump file with a name CrashDump.dmp. We will get the following message when the dump is in progress

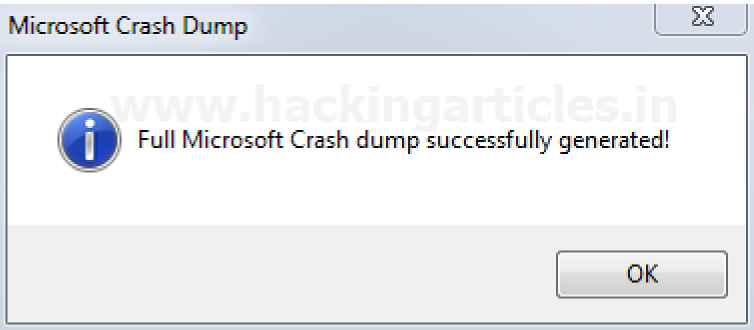


Microsoft Crash Dump

Generating crash dump.... this may take a few minutes

Please refrain from performing other activities while this dialog box is visible.

Once the dump is completed we will get a success message.



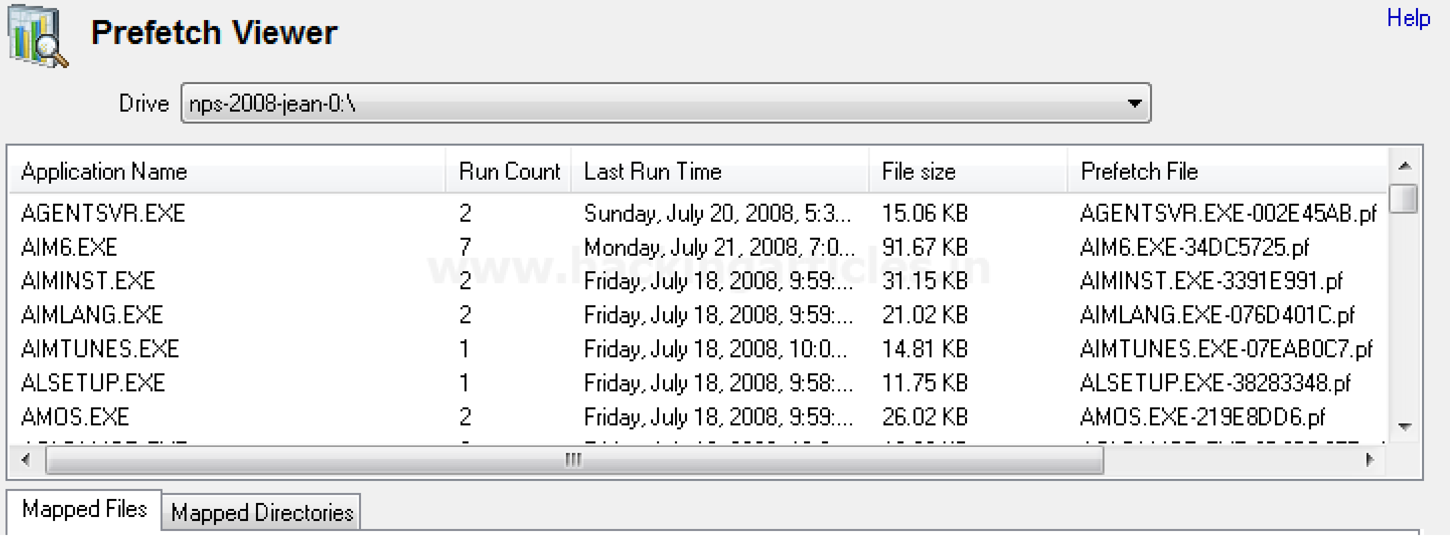
Microsoft Crash Dump

Full Microsoft Crash dump successfully generated!

This concludes the Memory Viewer

Prefetch Viewer

The prefetch viewer displays the .exe files that we have last executed on the system. To start with open OS Forensic and click on prefetch viewer.

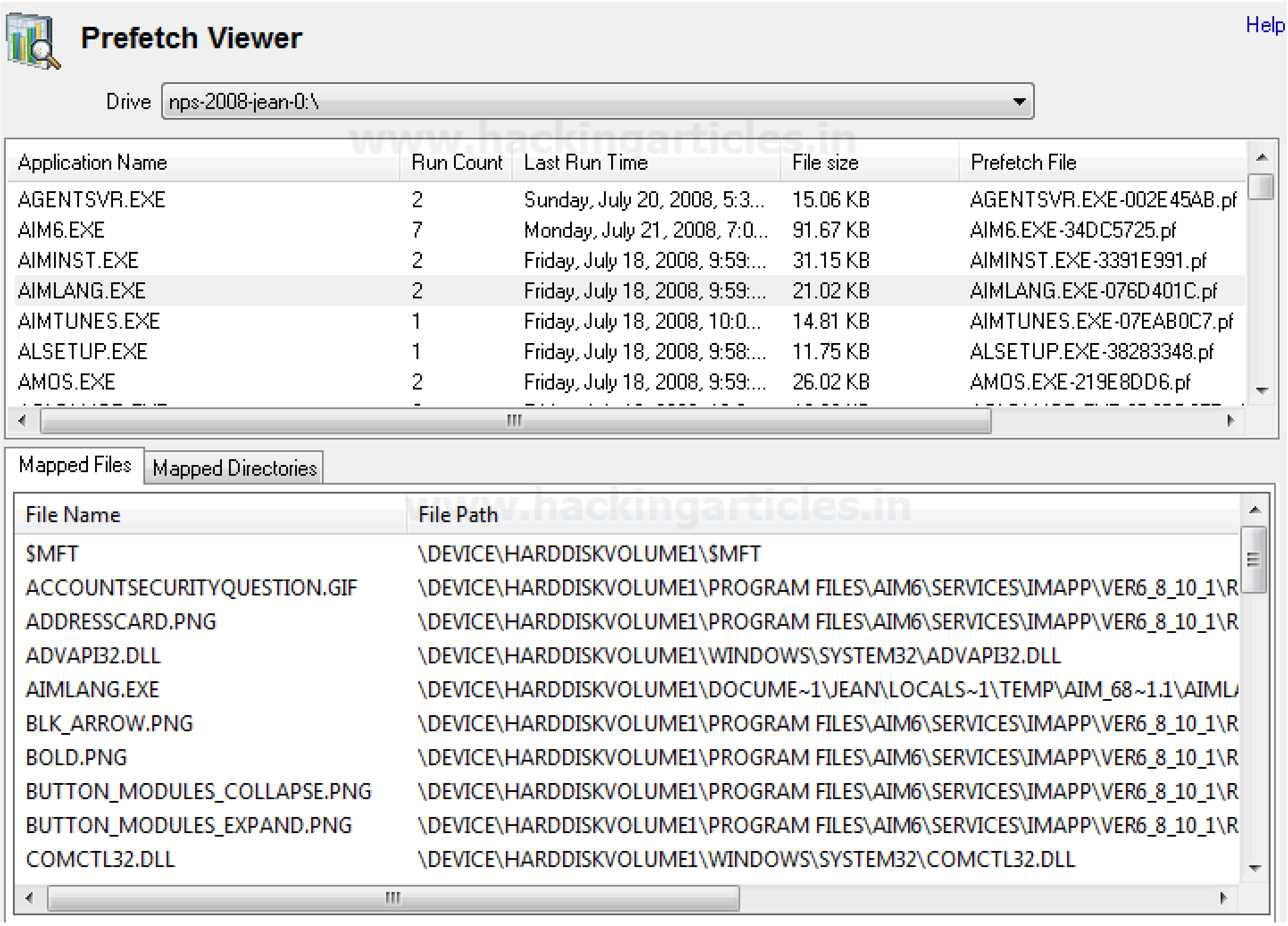


Prefetch Viewer

Drive nps-2008-jean-0:\

Application Name	Run Count	Last Run Time	File size	Prefetch File
AGENTSVR.EXE	2	Sunday, July 20, 2008, 5:3...	15.06 KB	AGENTSVR.EXE-002E45AB.pf
AIM6.EXE	7	Monday, July 21, 2008, 7:0...	91.67 KB	AIM6.EXE-34DC5725.pf
AIMINST.EXE	2	Friday, July 18, 2008, 9:59:...	31.15 KB	AIMINST.EXE-3391E991.pf
AIMLANG.EXE	2	Friday, July 18, 2008, 9:59:...	21.02 KB	AIMLANG.EXE-076D401C.pf
AIMTUNES.EXE	1	Friday, July 18, 2008, 10:0...	14.81 KB	AIMTUNES.EXE-07EAB0C7.pf
ALSETUP.EXE	1	Friday, July 18, 2008, 9:58:...	11.75 KB	ALSETUP.EXE-38283348.pf
AMOS.EXE	2	Friday, July 18, 2008, 9:59:...	26.02 KB	AMOS.EXE-219E8DD6.pf

We can browse the drive from the drop down to check the .exe file that has executed on a particular drive. We can click on any particular drive and can see the details of the exe along with mapped files under the mapped file tab.

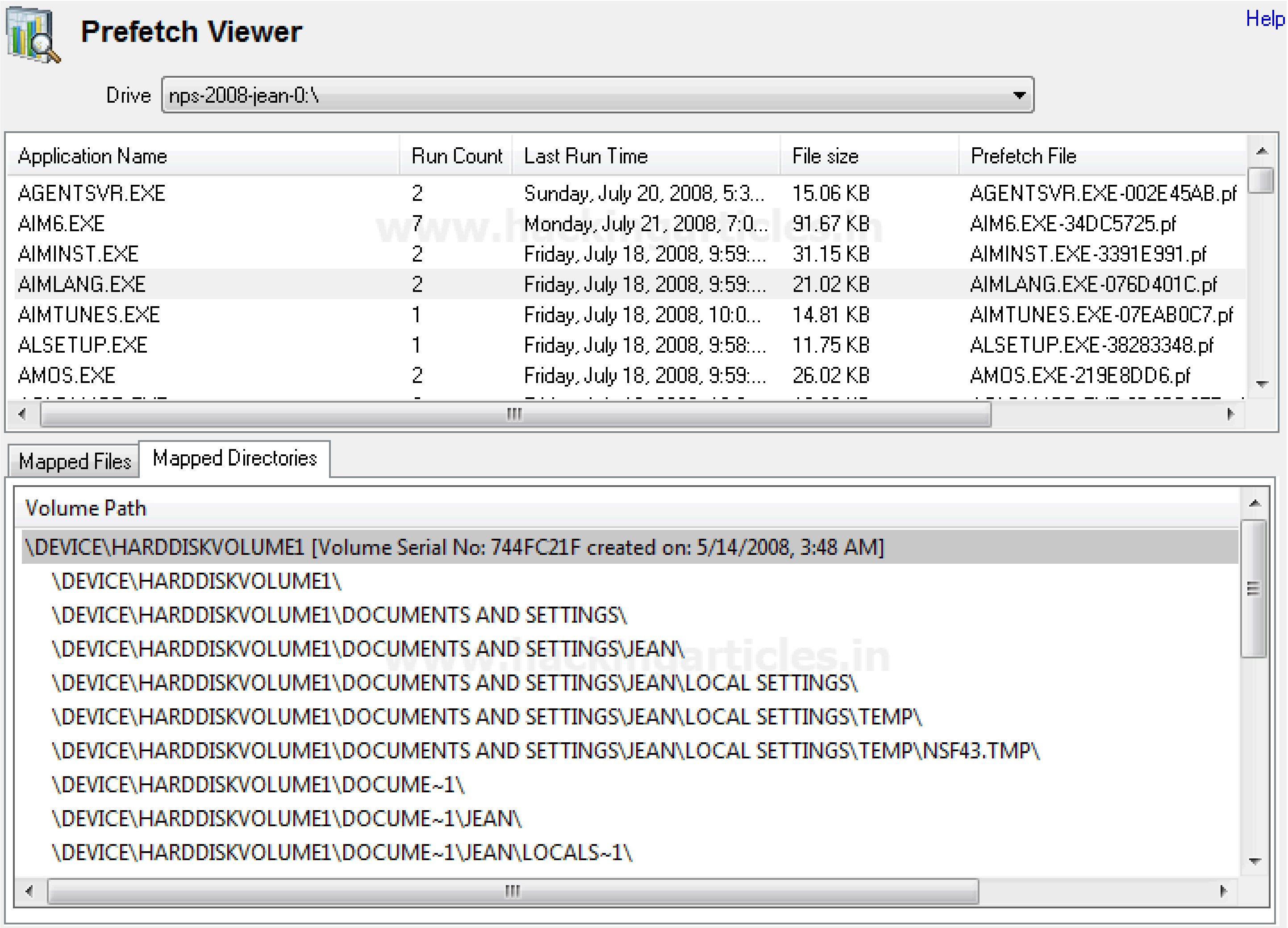


Drive: nps-2008-jean-0:\

Application Name	Run Count	Last Run Time	File size	Prefetch File
AGENTSVR.EXE	2	Sunday, July 20, 2008, 5:3...	15.06 KB	AGENTSVR.EXE-002E45AB.pf
AIM6.EXE	7	Monday, July 21, 2008, 7:0...	91.67 KB	AIM6.EXE-34DC5725.pf
AIMINST.EXE	2	Friday, July 18, 2008, 9:59:...	31.15 KB	AIMINST.EXE-3391E991.pf
AIMLANG.EXE	2	Friday, July 18, 2008, 9:59:...	21.02 KB	AIMLANG.EXE-076D401C.pf
AIMTUNES.EXE	1	Friday, July 18, 2008, 10:0...	14.81 KB	AIMTUNES.EXE-07EAB0C7.pf
ALSETUP.EXE	1	Friday, July 18, 2008, 9:58:...	11.75 KB	ALSETUP.EXE-38283348.pf
AMOS.EXE	2	Friday, July 18, 2008, 9:59:...	26.02 KB	AMOS.EXE-219E8DD6.pf

File Name	File Path
$MFT	\DEVICE\HARDDISKVOLUME1\$MFT
ACCOUNTSECURITYQUESTION.GIF	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\AIM6\SERVICES\IMAPP\VER6_8_10_1\R
ADDRESSCARD.PNG	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\AIM6\SERVICES\IMAPP\VER6_8_10_1\R
ADVAPI32.DLL	\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\ADVAPI32.DLL
AIMLANG.EXE	\DEVICE\HARDDISKVOLUME1\DOCUME~1\JEAN\LOCALS~1\TEMP\AIM_68~1.1\AIML
BLK_ARROW.PNG	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\AIM6\SERVICES\IMAPP\VER6_8_10_1\R
BOLD.PNG	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\AIM6\SERVICES\IMAPP\VER6_8_10_1\R
BUTTON_MODULES_COLLAPSE.PNG	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\AIM6\SERVICES\IMAPP\VER6_8_10_1\R
BUTTON_MODULES_EXPAND.PNG	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\AIM6\SERVICES\IMAPP\VER6_8_10_1\R
COMCTL32.DLL	\DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\COMCTL32.DLL

Also, we can view the directories, mapped with the .exe file under Mapped Directory Tab.



Application Name	Run Count	Last Run Time	File size	Prefetch File
AGENTSVR.EXE	2	Sunday, July 20, 2008, 5:3...	15.06 KB	AGENTSVR.EXE-002E45AB.pf
AIM6.EXE	7	Monday, July 21, 2008, 7:0...	91.67 KB	AIM6.EXE-34DC5725.pf
AIMINST.EXE	2	Friday, July 18, 2008, 9:59:...	31.15 KB	AIMINST.EXE-3391E991.pf
AIMLANG.EXE	2	Friday, July 18, 2008, 9:59:...	21.02 KB	AIMLANG.EXE-076D401C.pf
AIMTUNES.EXE	1	Friday, July 18, 2008, 10:0...	14.81 KB	AIMTUNES.EXE-07EAB0C7.pf
ALSETUP.EXE	1	Friday, July 18, 2008, 9:58:...	11.75 KB	ALSETUP.EXE-38283348.pf
AMOS.EXE	2	Friday, July 18, 2008, 9:59:...	26.02 KB	AMOS.EXE-219E8DD6.pf

```
Volume Path
\DEVICE\HARDDISKVOLUME1 [Volume Serial No: 744FC21F created on: 5/14/2008, 3:48 AM]
    \DEVICE\HARDDISKVOLUME1\
    \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\
    \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\JEAN\
    \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\JEAN\LOCAL SETTINGS\
    \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\JEAN\LOCAL SETTINGS\TEMP\
    \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\JEAN\LOCAL SETTINGS\TEMP\NSF43.TMP\
    \DEVICE\HARDDISKVOLUME1\DOCUME~1\
    \DEVICE\HARDDISKVOLUME1\DOCUME~1\JEAN\
    \DEVICE\HARDDISKVOLUME1\DOCUME~1\JEAN\LOCALS~1\
```

This concludes the Prefetch Viewer.

For more on OSForensics wait for the next article.