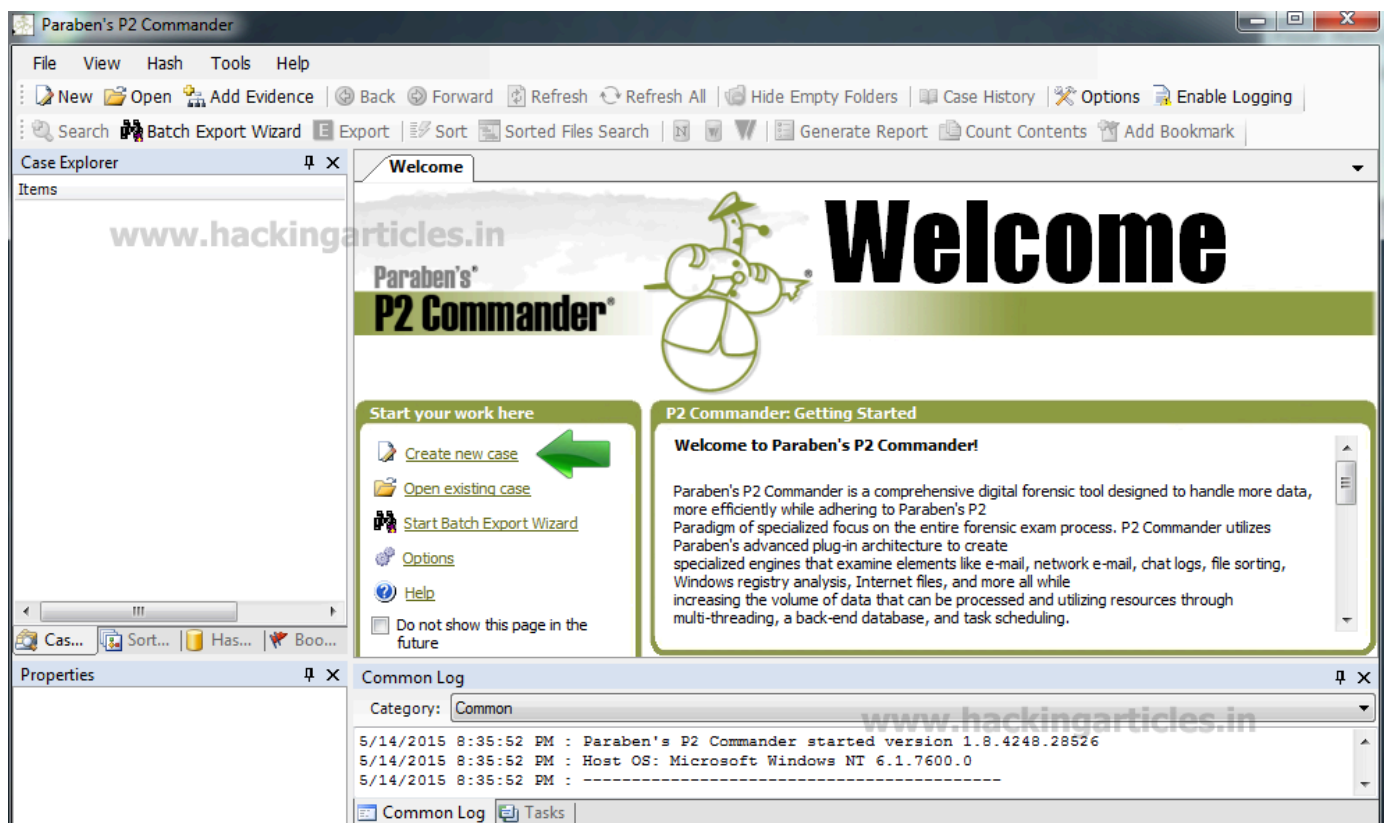


# How to Collect Forensics Evidence of PC using P2 Commander (Part 1)

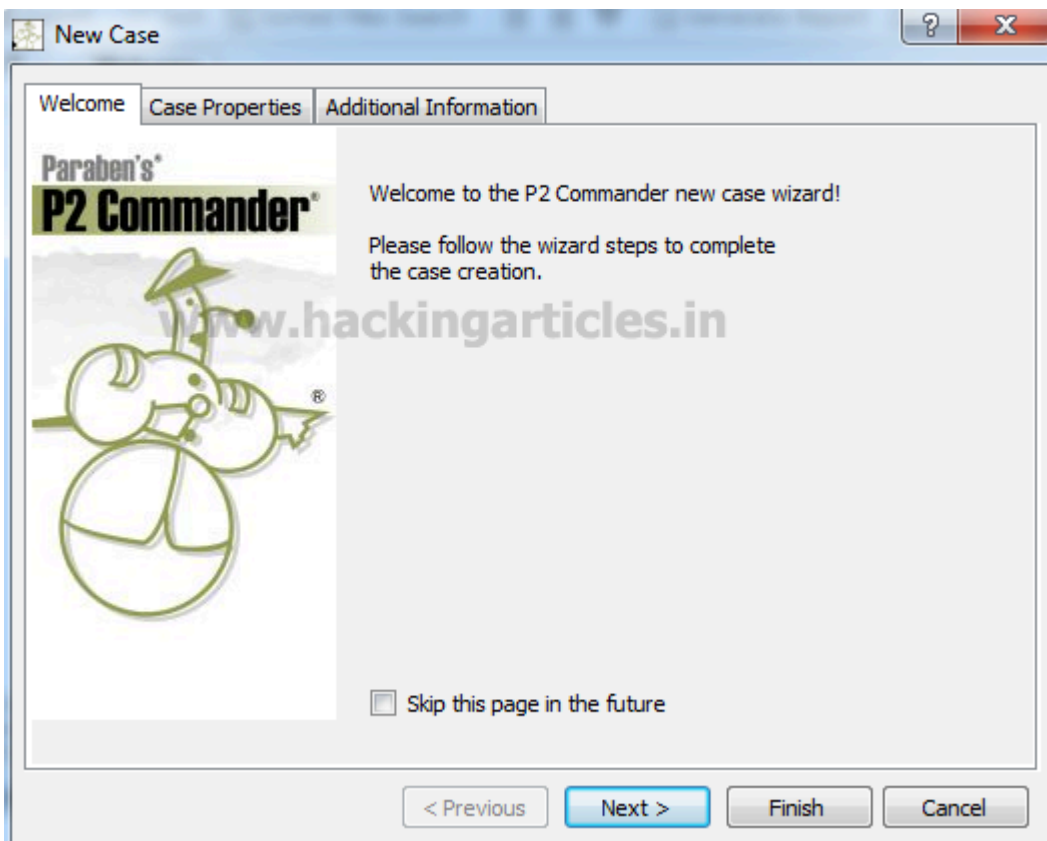
May 16, 2015 By Raj Chandel

P2C is a comprehensive digital investigation tool with over ten years of court-approved use by forensic examiners. An integrated database and true multi-threading mean faster processing. P2C was built on Paraben's trusted email examination tools for unparalleled network email and personal email archive analysis. Advanced features like Data Triage analysis, Xbox analysis, pornography detection.

First Download the p2 commander from [here](#) and install in victim pc and open p2 commander Click **New Case** the 'Create a New Case' page will open



Then click on **next** to proceed to next step.



Here in next step you have to enter the **case name** and **DEMO** details and click on **finish** to proceed to next step

This is a screenshot of the 'New Case' wizard window, specifically the 'Case Properties' tab. The window has the same title bar and tabs as the previous screenshot. The 'Case Properties' tab is active, showing the title 'Case Properties' and a note: 'Please enter the case properties. Please note that the field "Case name" is required.' There is a small icon of the cartoon character in the top right corner. Below the note, there is a text input field for 'Case name:' with the text 'DEMO' entered. Below that is a text area for 'Description :' with the text 'Practice' entered. At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'. A watermark 'www.hackingarticles.in' is visible across the center.

Here in next step you have to enter the **Investigator name** and **email** details and click on **finish** to proceed to next step

The screenshot shows a 'New Case' dialog box with three tabs: 'Welcome', 'Case Properties', and 'Additional Information'. The 'Additional Information' tab is active. It contains a title bar with a question mark and a close button. Below the tabs, there is a section titled 'Additional Information' with a small icon of a person. The text below the title says: 'Please enter additional information. This information is not required and can be filled any time through the Properties pane.' The form contains several fields: 'Investigator name:' with a dropdown menu showing 'Raj Chandel'; 'Agency/Company:' with a dropdown menu showing 'Hacking Articles'; 'Phone:' and 'Fax:' with empty text boxes; 'Address:' with an empty text box; 'E-mail:' with a dropdown menu showing 'raj@hackingarticles.in'; and 'Comments:' with a large empty text area. At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish' (highlighted with a blue border), and 'Cancel'. A watermark 'www.hackingarticles.in' is visible across the center of the form.

**New Case**

Welcome Case Properties **Additional Information**

**Additional Information**

Please enter additional information. This information is not required and can be filled any time through the Properties pane.

Investigator name: Agency/Company:

Raj Chandel Hacking Articles

Phone: Fax:

Address: E-mail:

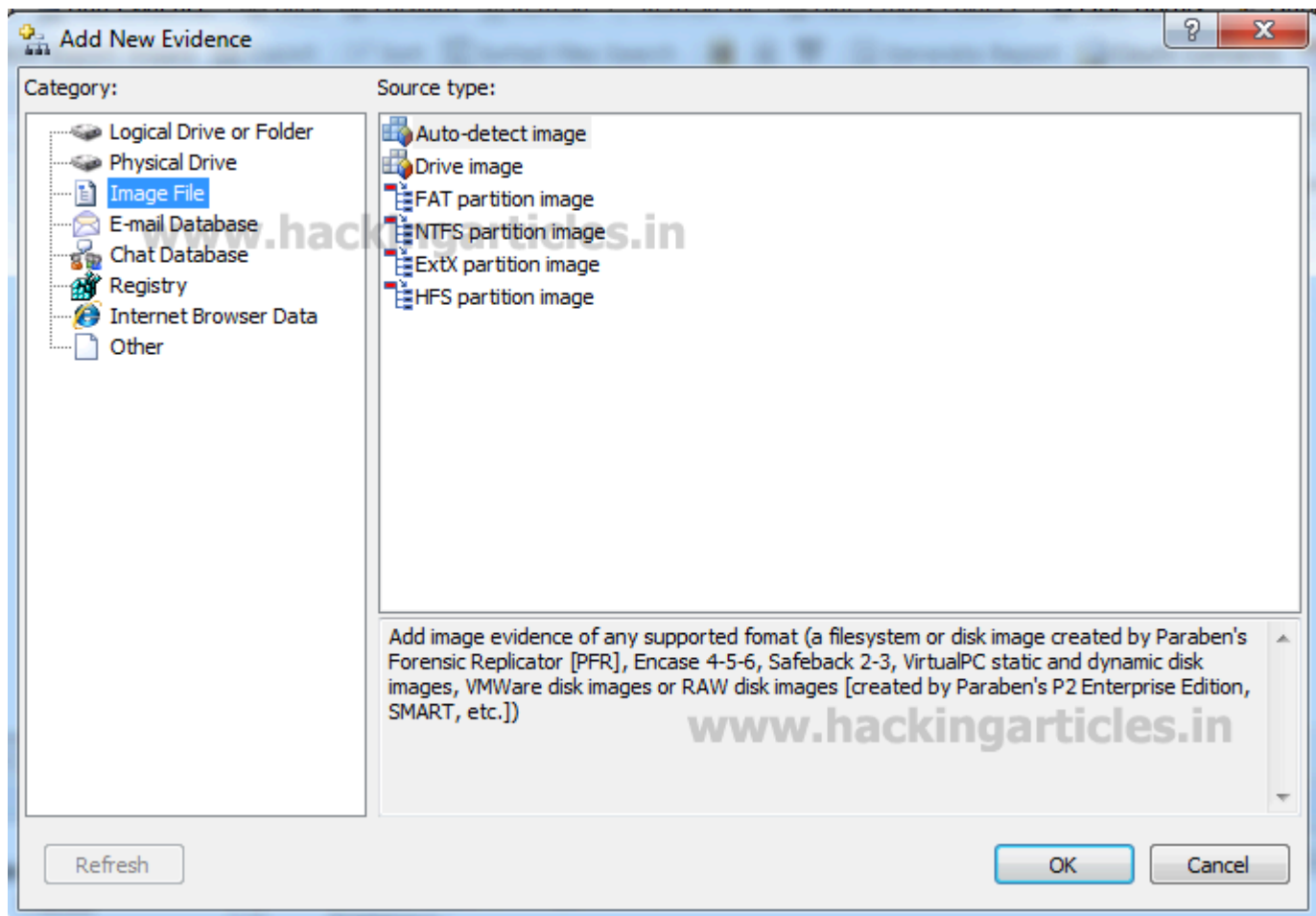
raj@hackingarticles.in

Comments:

< Previous Next > Finish Cancel

Now Click '**Add Evidence**'->Choose '**Image File**'

Now select **Auto-detect Image** option from **source type** which will add the image evidence in any format. You can choose any option from different available options such as Drive Image or Fat Partition Image.

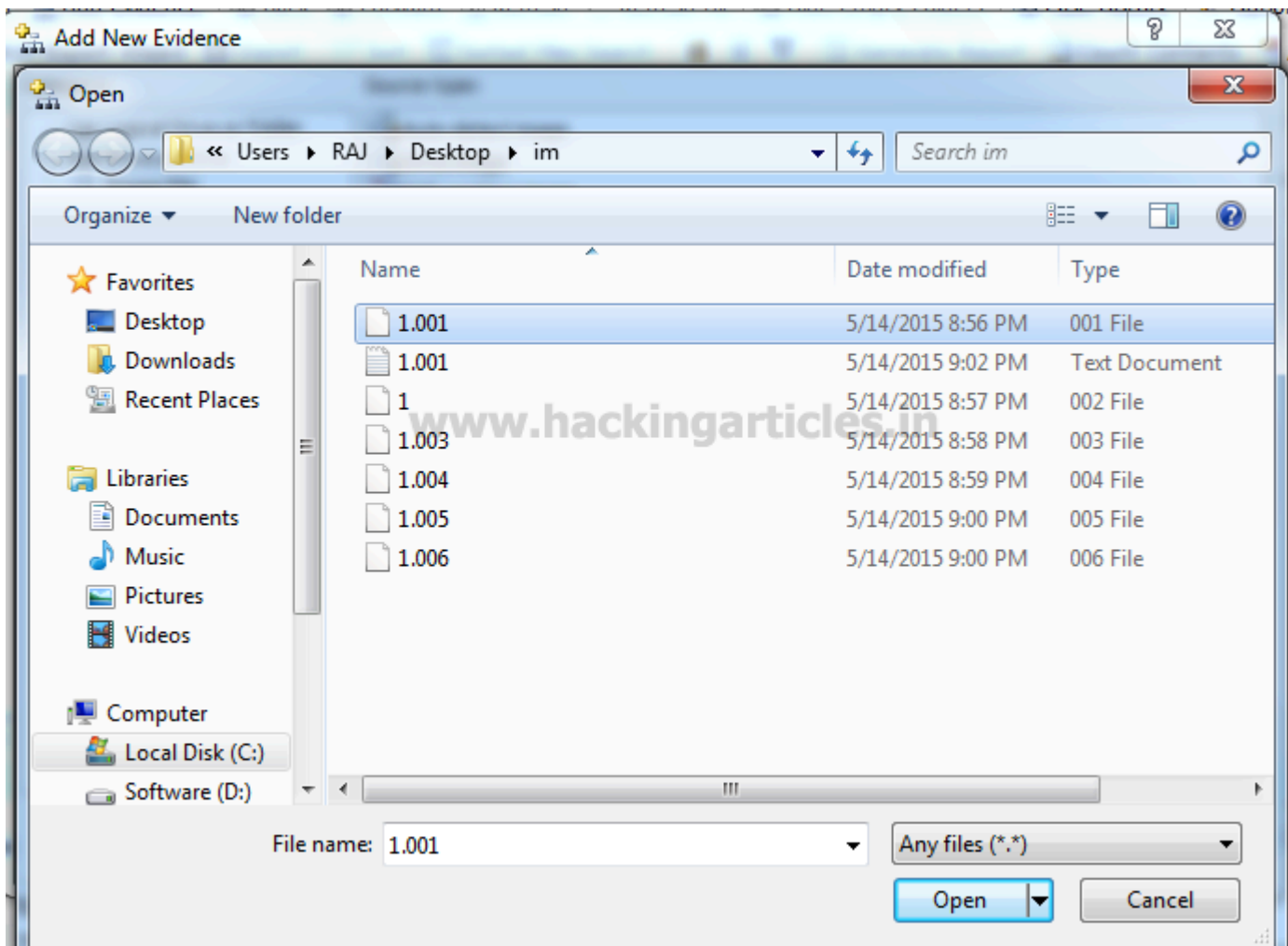


Now load the Evidence Disk Image

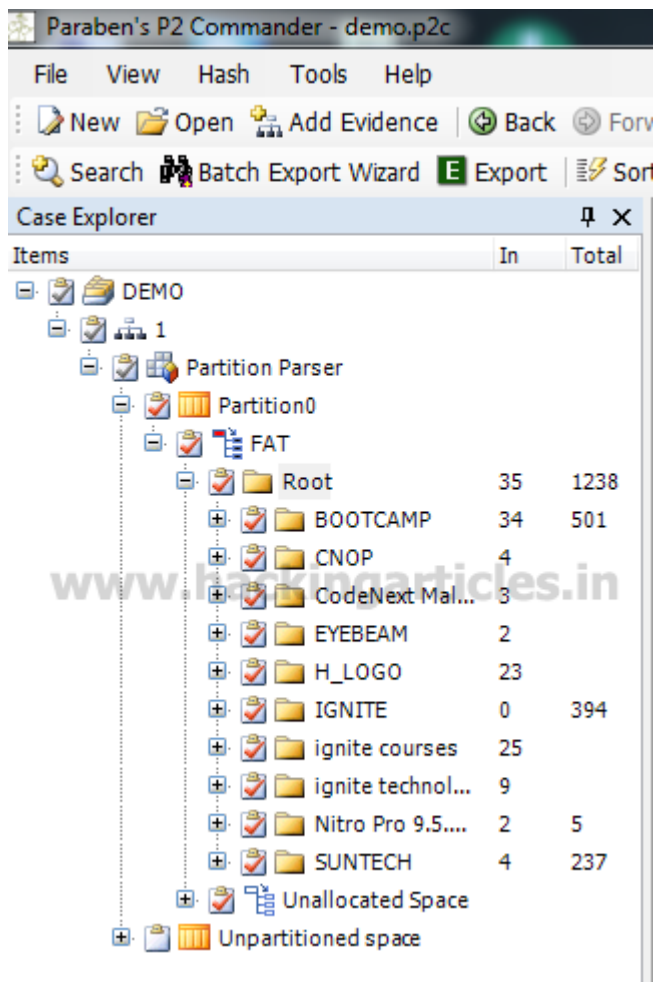
**How to create Disk Image read this article**

**<http://www.hackingarticles.in/how-to-create-copy-of-suspects-evidence-using-ftk-imager/>**

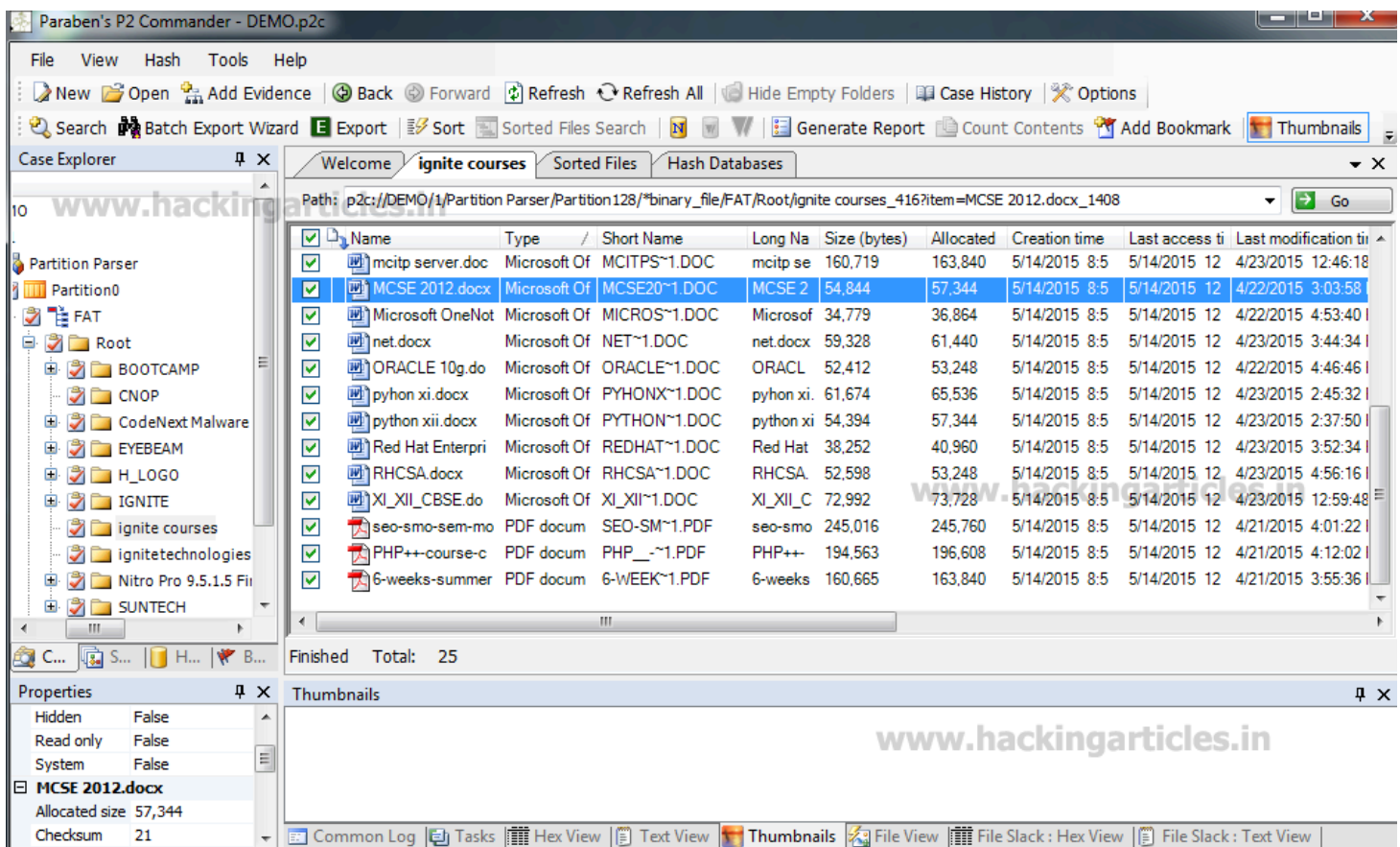
After selecting the evidence Image, click on **Open**.



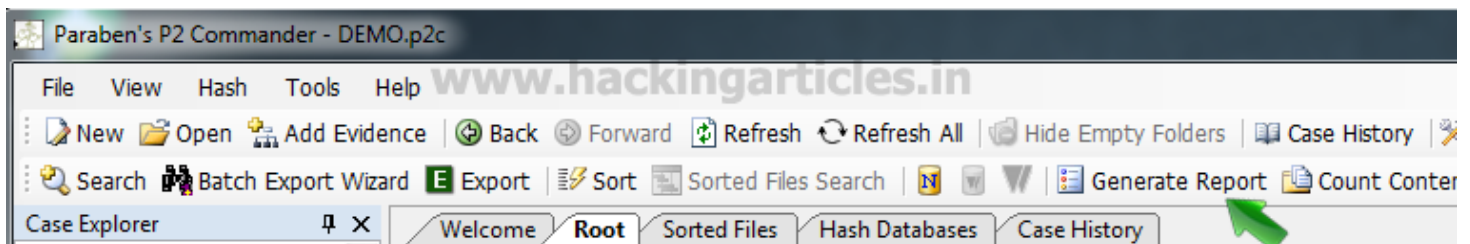
Now you will see the case **Demo** is created, which will show you the hierarchy of the directories of the evidence image.



Now you can click on any one of the directories of the evidence image and it will show you all the containing files and sub folders within that folder describing their file name, file type, file size, creation time and last modification etc.



Now click on **generate report** tab.



Select the report type which is to be generated. In my case I am selecting **HTML Investigative Report** & select the destination folder. Then click on **next**.

Reports Wizard

### General options

Select General options: report type, destination folder etc. Follow the wizard steps to define what information will be added to the report.

**General options**

- Investigator's Information
- Filesystem types
  - File properties
- Types of Sorted files
- Other evidence
- Logs & Supplementary files

Select the report type to be generated :

☒ HTML Investigative Report [\(example\)](#)

☐ Simple Text Report [\(example\)](#)

☐ CSV Text Report [\(example\)](#)

☐ HTML Evidence Summary Report [\(example\)](#)

☐ HTML E-mail Message Report [\(example\)](#)

☒ Include detected virtual file system databases

Destination folder :

C:\Users\RAJ\Desktop\Reports\ [Browse...](#)

NOTE: the folder should be empty, otherwise all data stored in it will be lost.  
Please make sure there is enough room for the exported files.

☐ Open report on finish

☐ Save current wizard options as default

< Previous    Next >    Finish    Cancel

Now select the sorted file which is to be added by clicking on Add and Export button with their file types. Now click on next to proceed further.



Reports Wizard

### Filesystem types

Select what types of sorted files will be added to the report.

General options  
Investigator's Information  
**Filesystem types**  
- File properties  
Types of Sorted files  
Other evidence  
Logs & Supplementary files

☒ Include only data checked as "Include to reports"  
☐ Include all filesystem evidence files of the selected types  
☐ Don't include filesystem evidence

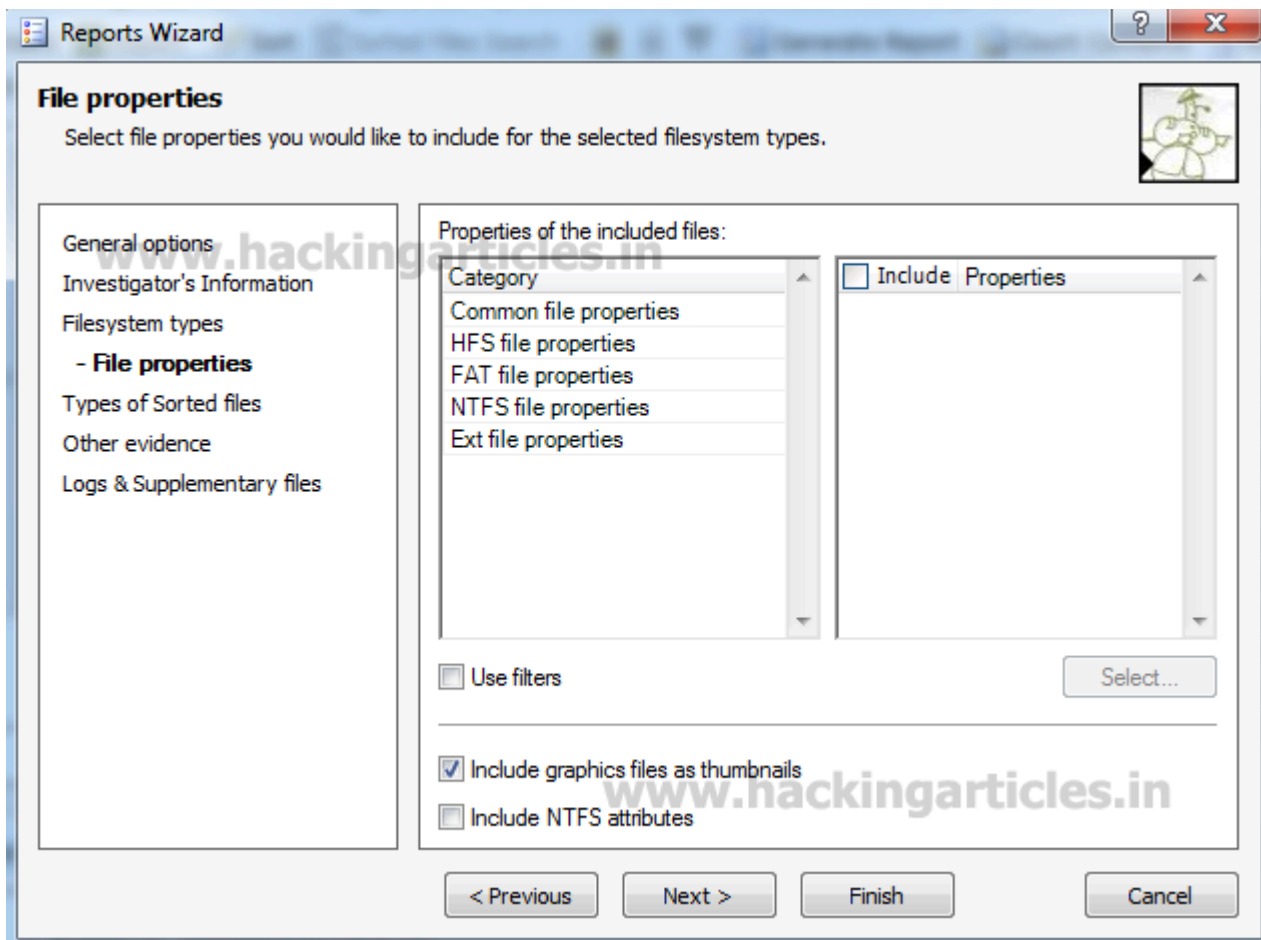
Check the Add checkbox to add a file's data to the report. Check the Export checkbox to export a file's data and add links to the report.

<input checked="" type="checkbox"/> Add	<input checked="" type="checkbox"/> Export	File types
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Documents
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Email
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Chats
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Spreadsheets
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Graphics
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Databases
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Executable
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Compressed

☐ Show data by file types (Only for sorted data)  
☒ Show data in tree-view structure (Case Explorer)

< Previous    Next >    Finish    Cancel

Now click on **Finish** to proceed to next step.



The report file will be saved on your destination folder. Now you will visualize the details of your report.

