How to gather Forensics Investigation Evidence using ProDiscover Basic

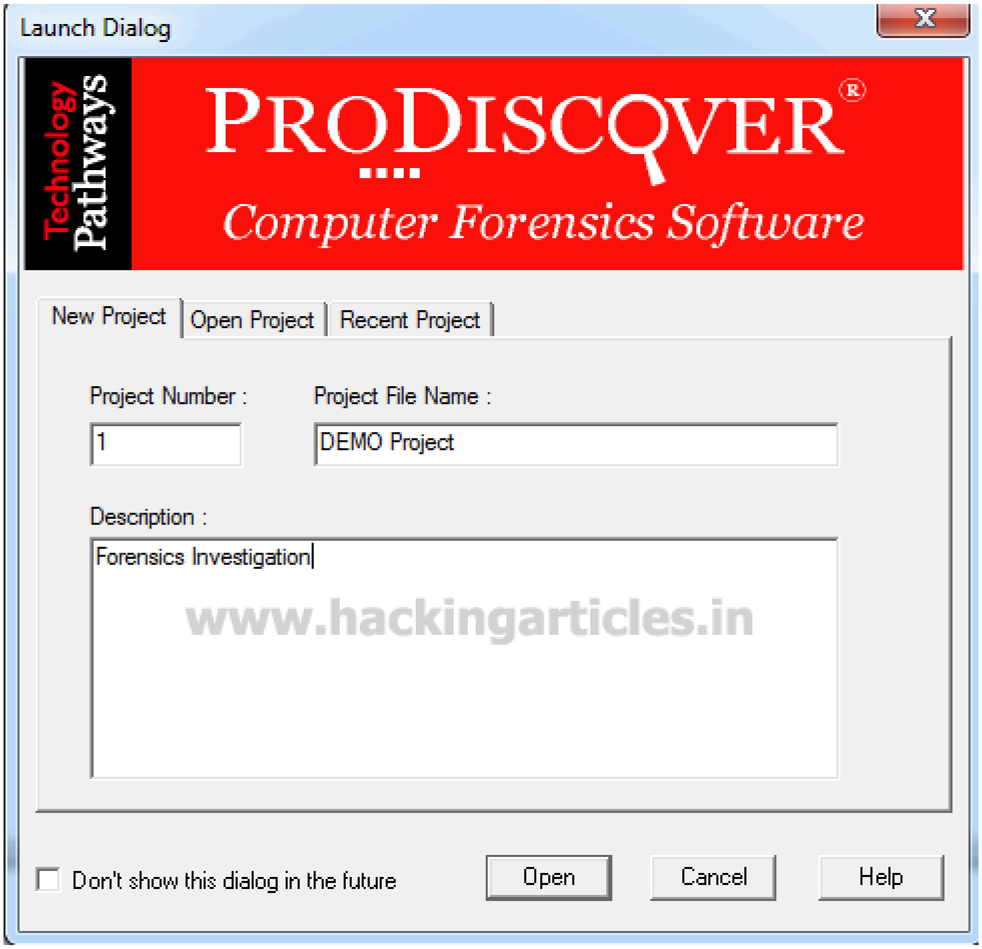
May 19, 2015 By Raj Chandel

The ARC Group ProDiscover® Basic edition is a self-managed tool for the examination of your hard disk security. ProDiscover Basic is designed to operate under the National Institute of Standards' Disk Imaging Tool Specification 3.1.6 to collect snapshots of activities that are critical to taking proactive steps in protecting your data.

ProDiscover Basic has a built-in reporting tool to present findings as evidence for legal proceedings. You gather time zone data, drive information, Internet activity, and more, piece by piece, or in a full report as needed. You have robust search capabilities for capturing unique data, filenames and filetypes, data patterns, date ranges, etc. ProDiscover Basic gives clients the autonomy they desire in managing their own data security.

At the ARC Group, we provide the tools you need to identify security issues before they escalate, and we use ProDiscover solutions to maintain your corporate safety and preserve your data. With ProDiscover Basic, professional consultants, system administrators, and investigators take the upper hand to manage cyber security at every level and protect information in the case of impending legal actions.

First Download the **ProDiscover Basic** from **here** and install it in pc and enter the **Project Number**, **Project File Name** and **Description** in **prodiscover basic** software**.** Click on **Open**.



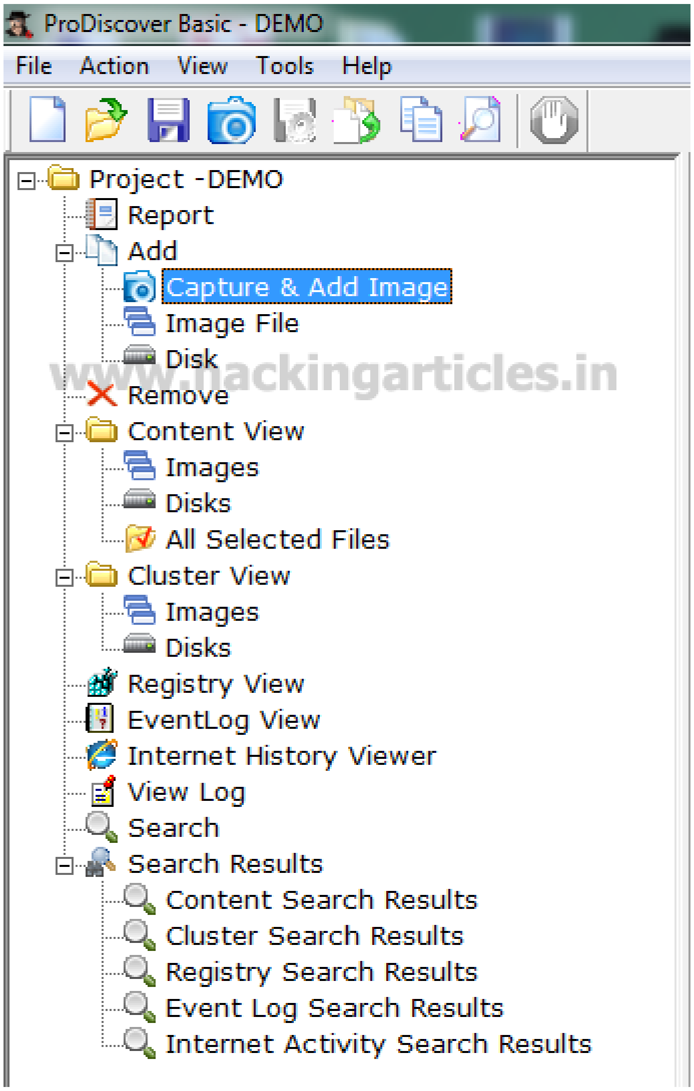
Project Number : 1

Project File Name : DEMO Project

Description : Forensics Investigation

□ Don't show this dialog in the future

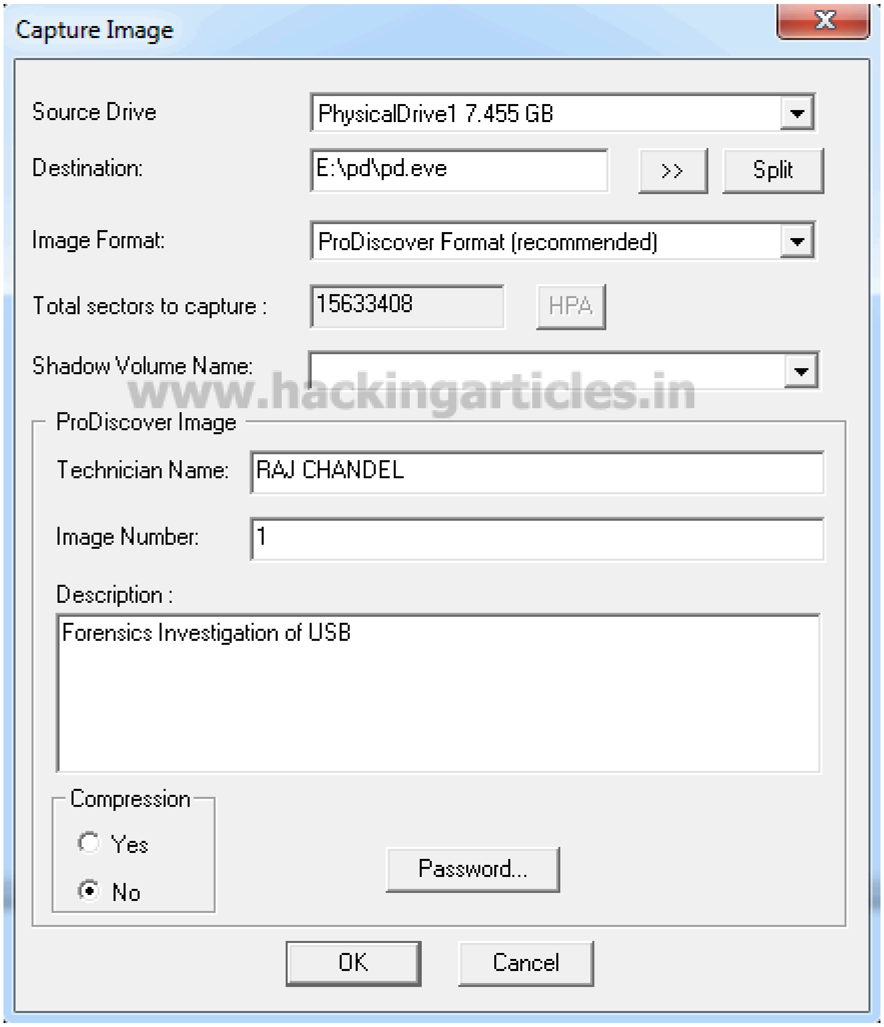
In main window click on **Capture & Add Image**



Now select the source drive that we want to capture, this could be a USB Drive or physical Drive.In my case I select drive **Physical Drive 1** which is my USB drive.

Now set the destination of the image file where we want to store it, in my case I used **E:** drive and named the image folder as pd and the name of the image which is to be saved in desired folder is PD.EVE .

Now enter the '**Technician Name'**, '**Image Number'** and '**description'** Now Click on ok.



Source Drive: PhysicalDrive1 7.455 GB

Destination: E:\pd\pd.eve

Image Format: ProDiscover Format (recommended)

Total sectors to capture : 15633408

Shadow Volume Name:

ProDiscover Image

Technician Name: RAJ CHANDEL

Image Number: 1

Description : Forensics Investigation of USB

Compression
○ Yes
● No

After finishing the following steps, windows will appear.

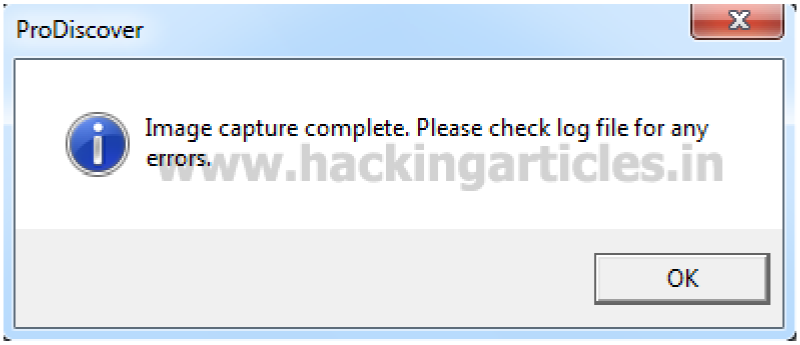
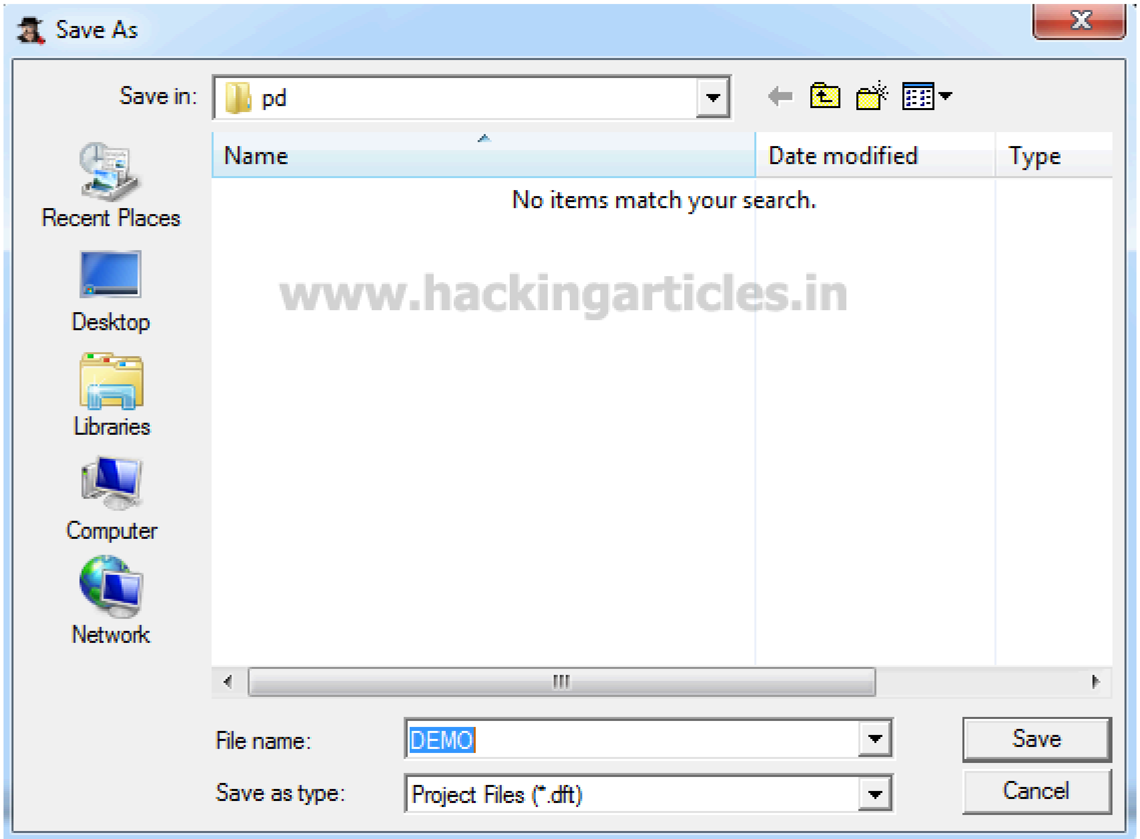


Image capture complete. Please check log file for any errors.

After imaging the drive close the **prodiscover** program then it will ask you to save your project.



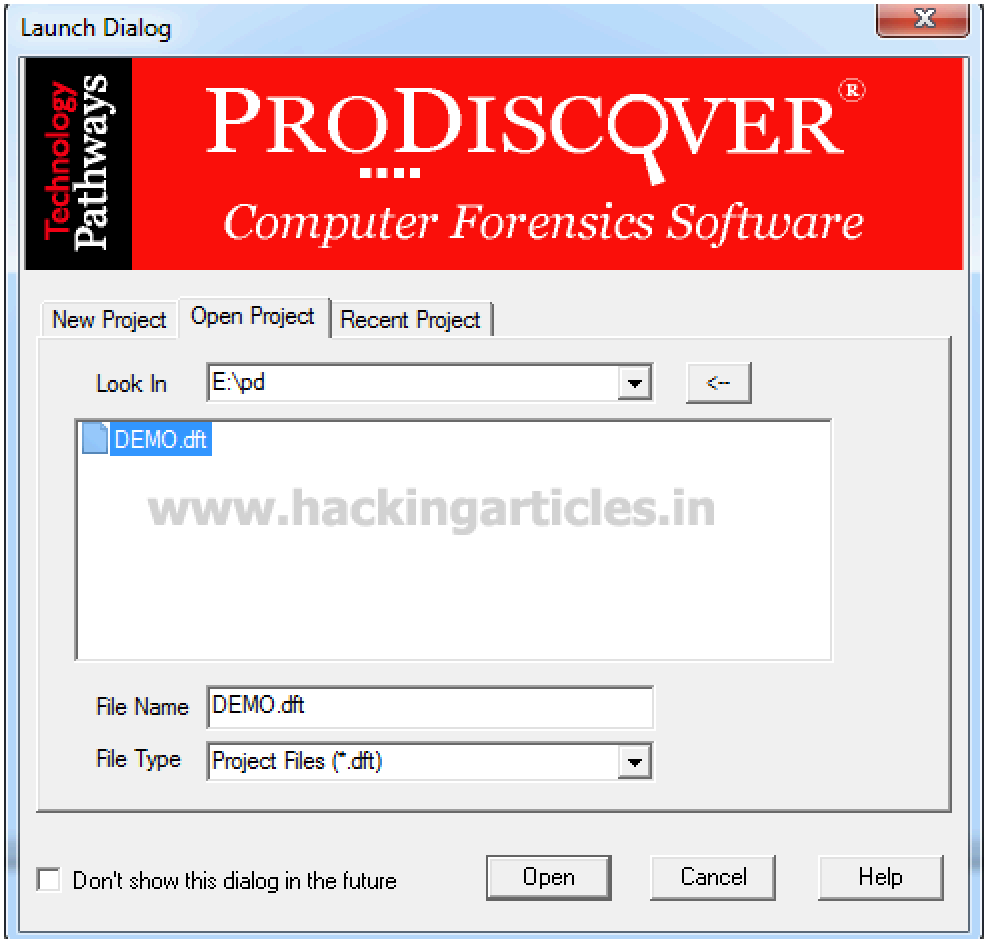
Save in: pd

No items match your search.

File name: DEMO

Save as type: Project Files (*.dft)

Now starts prodiscover program again and click on **open project** and browser your project image select it and click **open**



Look In: E:\pd

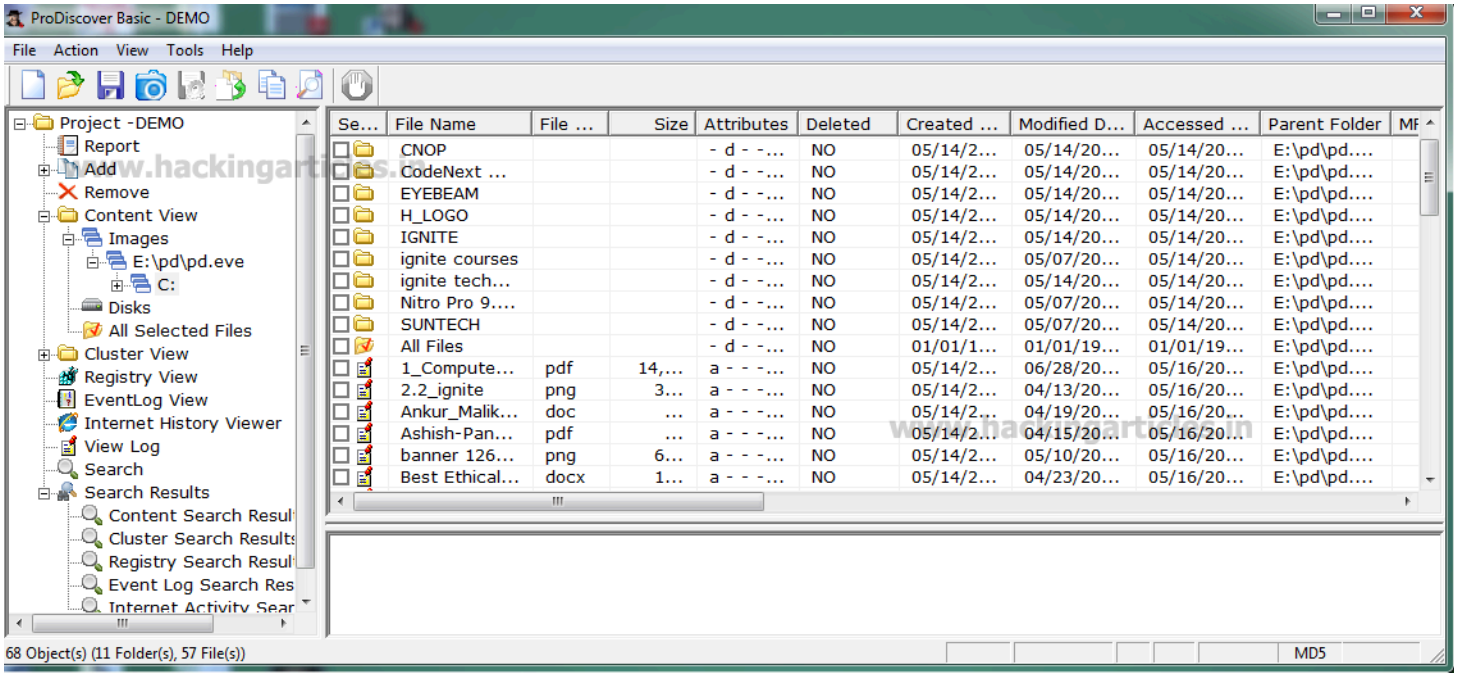
DEMO.dft

File Name: DEMO.dft

File Type: Project Files (*.dft)

□ Don't show this dialog in the future

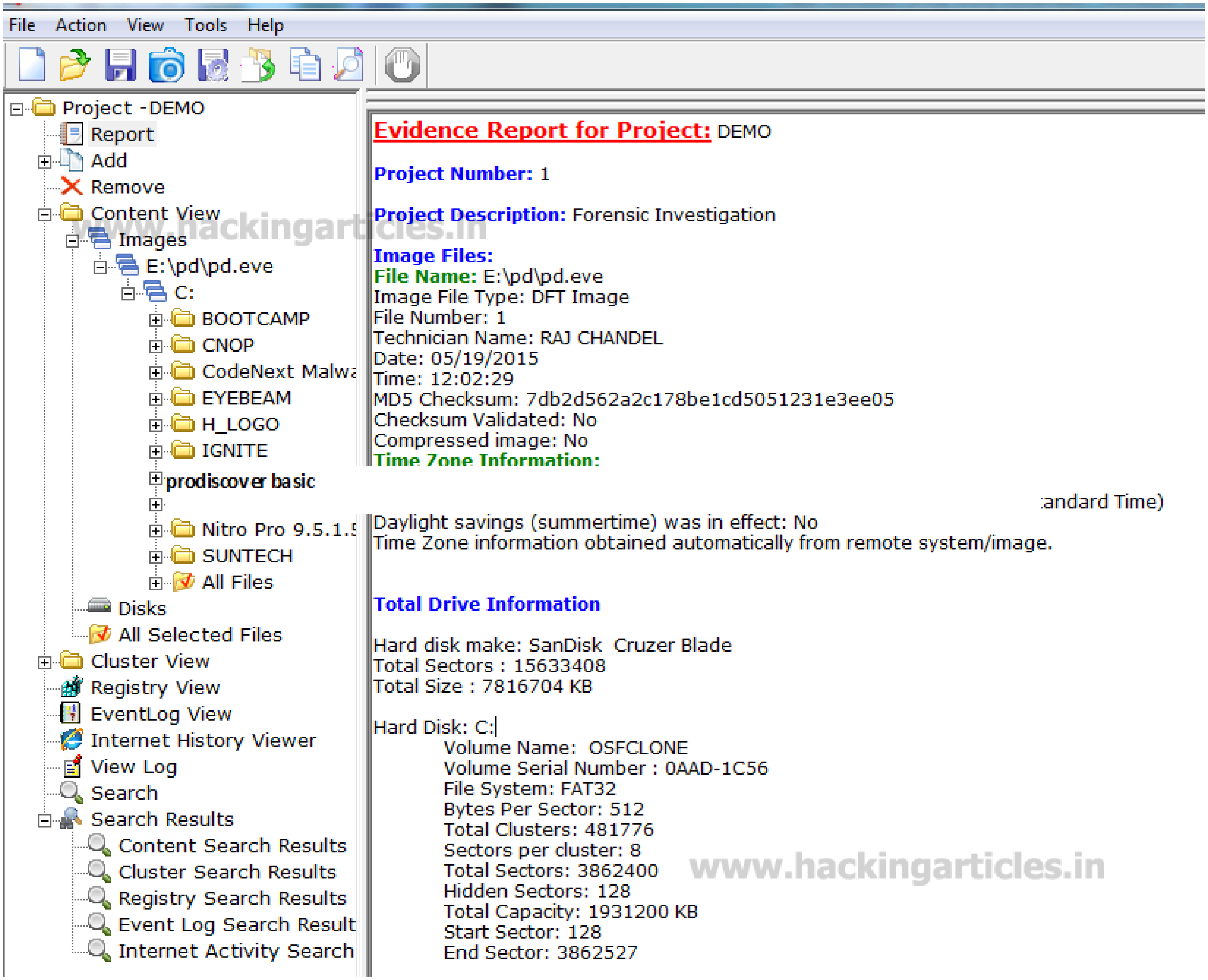
Now the project will open & go to the left menu and click on **Content View.** Then it will show you all the contents of evidence image.



Se...	File Name	File ...	Size	Attributes	Deleted	Created ...	Modified D...	Accessed ...	Parent Folder	MF
☐	CNOP			- d - -...	NO	05/14/2...	05/14/20...	05/14/20...	E:\pd\pd....	
☐	CodeNext ...			- d - -...	NO	05/14/2...	05/14/20...	05/14/20...	E:\pd\pd....	
☐	EYEBEAM			- d - -...	NO	05/14/2...	05/14/20...	05/14/20...	E:\pd\pd....	
☐	H_LOGO			- d - -...	NO	05/14/2...	05/14/20...	05/14/20...	E:\pd\pd....	
☐	IGNITE			- d - -...	NO	05/14/2...	05/14/20...	05/14/20...	E:\pd\pd....	
☐	ignite courses			- d - -...	NO	05/14/2...	05/07/20...	05/14/20...	E:\pd\pd....	
☐	ignite tech...			- d - -...	NO	05/14/2...	05/14/20...	05/14/20...	E:\pd\pd....	
☐	Nitro Pro 9....			- d - -...	NO	05/14/2...	05/07/20...	05/14/20...	E:\pd\pd....	
☐	SUNTECH			- d - -...	NO	05/14/2...	05/07/20...	05/14/20...	E:\pd\pd....	
☐	All Files			- d - -...	NO	01/01/1...	01/01/19...	01/01/19...	E:\pd\pd....	
☐	1_Compute...	pdf	14,...	a - - -...	NO	05/14/2...	06/28/20...	05/16/20...	E:\pd\pd....	
☐	2.2_ignite	png	3...	a - - -...	NO	05/14/2...	04/13/20...	05/16/20...	E:\pd\pd....	
☐	Ankur_Malik...	doc	...	a - - -...	NO	05/14/2...	04/19/20...	05/16/20...	E:\pd\pd....	
☐	Ashish-Pan...	pdf	...	a - - -...	NO	05/14/2...	04/15/20...	05/16/20...	E:\pd\pd....	
☐	banner 126...	png	6...	a - - -...	NO	05/14/2...	05/10/20...	05/16/20...	E:\pd\pd....	
☐	Best Ethical...	docx	1...	a - - -...	NO	05/14/2...	04/23/20...	05/16/20...	E:\pd\pd....	

68 Object(s) (11 Folder(s), 57 File(s))

To generate the automatic report click on **report** tab under the **view** menu. Then it will show you Evidence Report.



Evidence Report for Project: DEMO

Project Number: 1

Project Description: Forensic Investigation

Image Files:
File Name: E:\pd\pd.eve
Image File Type: DFT Image
File Number: 1
Technician Name: RAJ CHANDEL
Date: 05/19/2015
Time: 12:02:29
MD5 Checksum: 7db2d562a2c178be1cd5051231e3ee05
Checksum Validated: No
Compressed image: No
Time Zone Information:

:andard Time)
Daylight savings (summertime) was in effect: No
Time Zone information obtained automatically from remote system/image.

Total Drive Information

Hard disk make: SanDisk Cruzer Blade
Total Sectors : 15633408
Total Size : 7816704 KB

Hard Disk: C:
    Volume Name: OSFCLONE
    Volume Serial Number : 0AAD-1C56
    File System: FAT32
    Bytes Per Sector: 512
    Total Clusters: 481776
    Sectors per cluster: 8
    Total Sectors: 3862400
    Hidden Sectors: 128
    Total Capacity: 1931200 KB
    Start Sector: 128
    End Sector: 3862527