

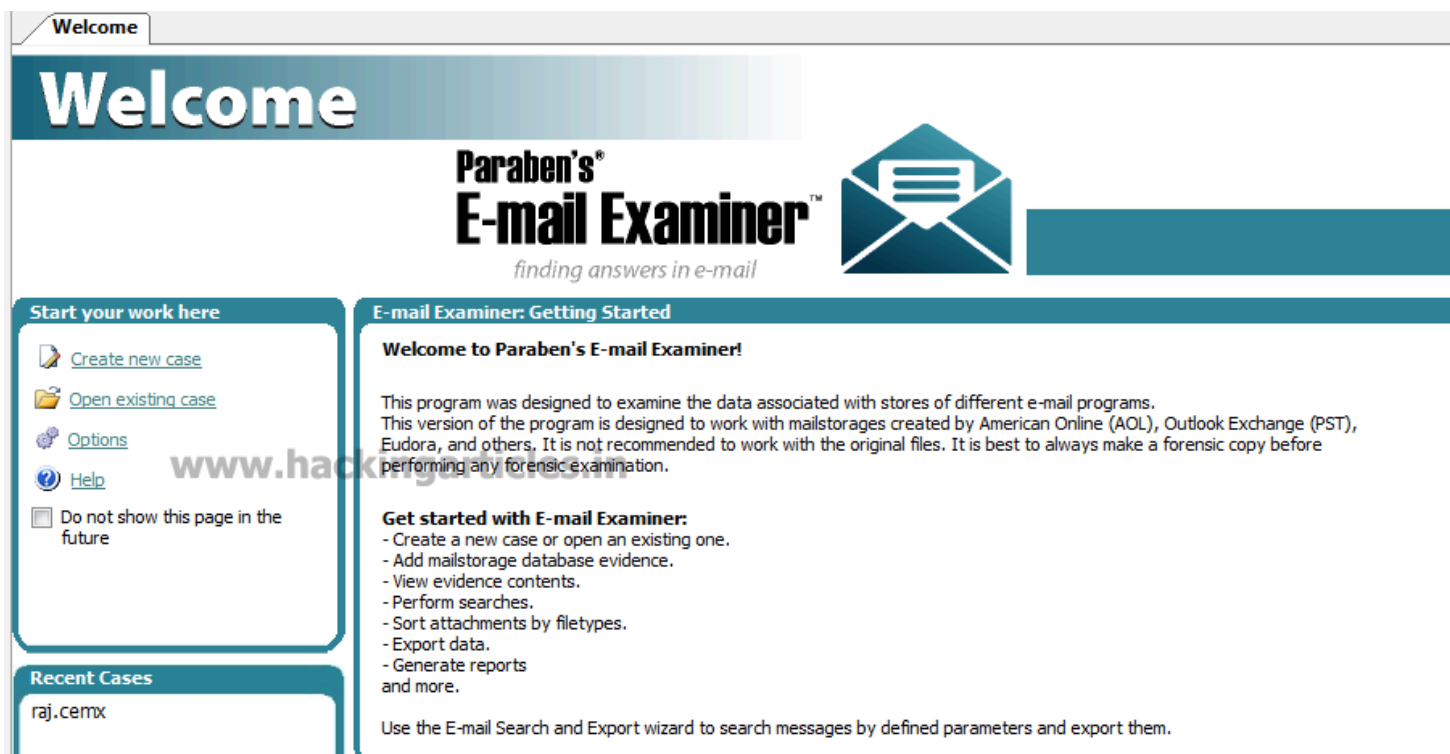
Outlook Forensics Investigation using E-Mail Examiner

June 2, 2015 By Raj Chandel

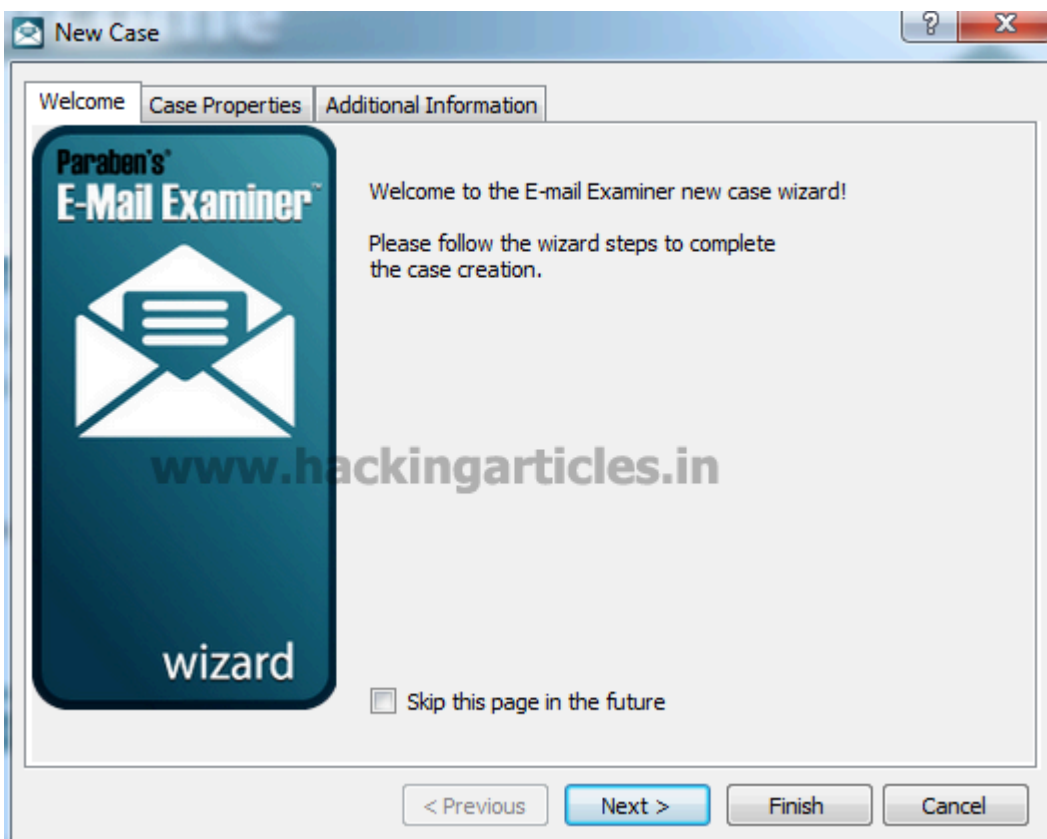
Forensically examine hundreds of email formats including Outlook (PST and OST), Thunderbird, Outlook Express, Windows mail, and more. Paraben's Email Examiner is one of the most comprehensive forensically sound email examination tools available. Email Examiner allows you to analyze message headers, bodies, and attachments. Email Examiner doesn't just recover email in the deleted folders; it recovers email deleted from deleted items.

- Microsoft Outlook (PST)
- Microsoft Outlook Offline Storage (OST)
- America On-line (AOL)
- The Bat! (version 3.x and higher)
- Thunderbird
- Outlook Express
- Eudora
- Email file – RFC 833 Compliant(EML)
- Windows mail databases
- Maildir
- Plain Text mail
- Support for more than 750 MIME Types

First Download the E-Mail Examiner from **here** and install in victim pc and open E-Mail Examiner Click on **'Create a New Case' option.**



New Case window will be open. Then click on **next** to proceed to next step.



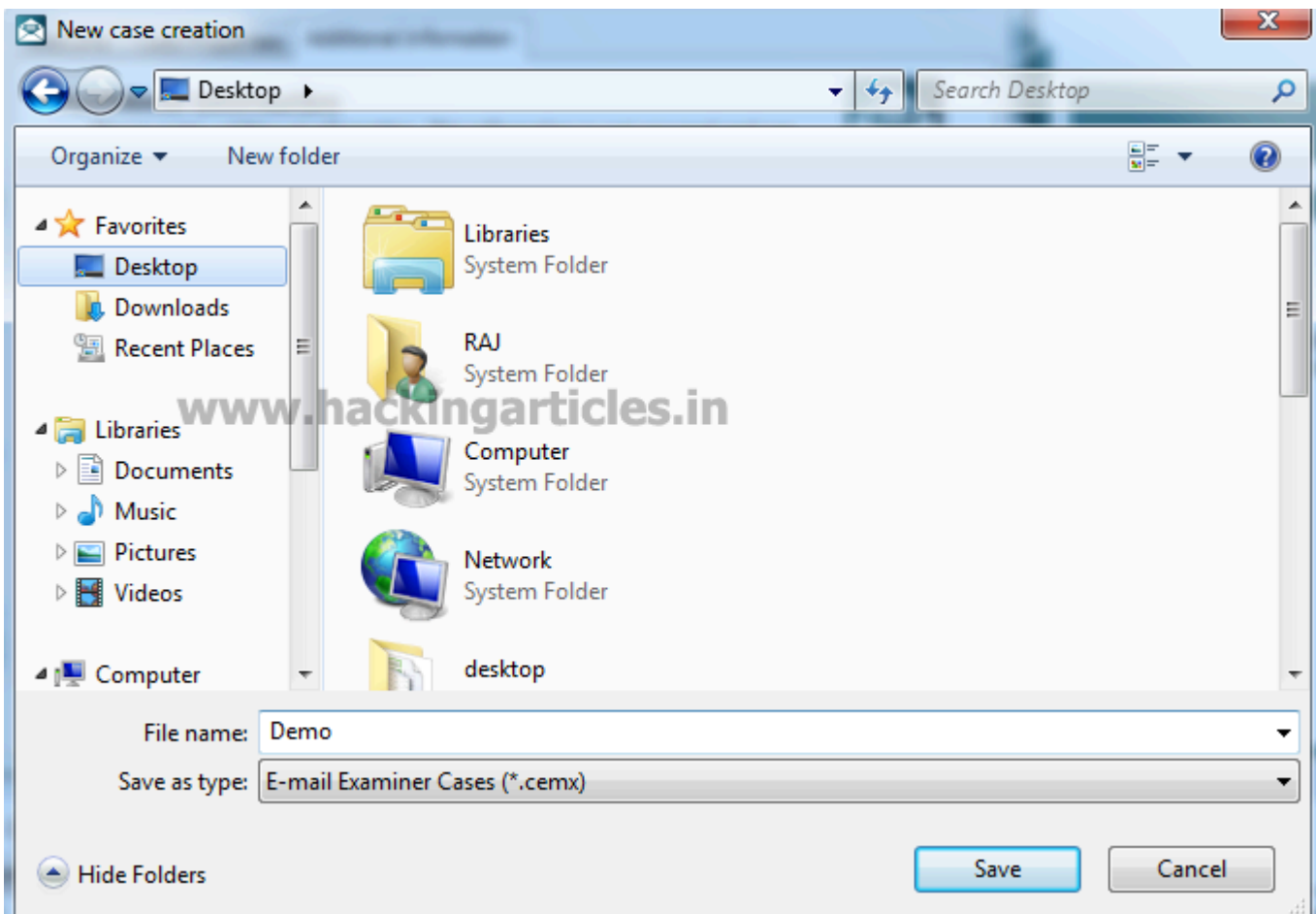
Here in next step you have to enter the **case name** as **DEMO** and **description** details and click on **finish** to proceed to next step.

The screenshot shows a window titled 'New Case' with three tabs: 'Welcome', 'Case Properties', and 'Additional Information'. The 'Case Properties' tab is active. It contains a message: 'Please enter case properties. The Case name field is required.' Below this, there is a 'Case name:' label and a text box containing 'Demo'. A 'Description:' label is followed by a large text area containing 'Email Forensics Investigation'. At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'. A watermark 'www.hackingarticles.in' is visible across the center.

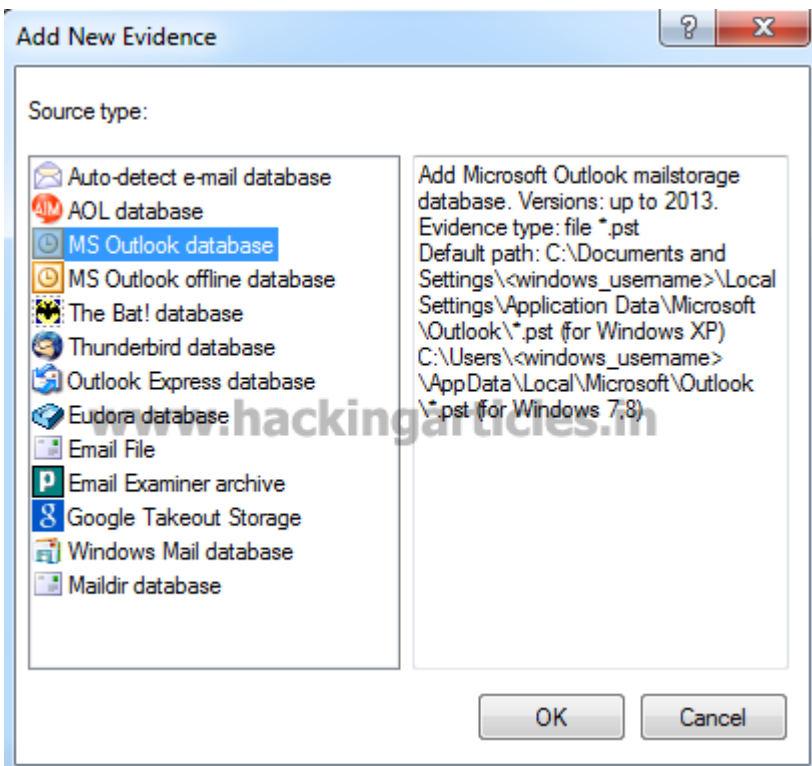
Here in next step you have to enter the **Investigator name** and **email details** and click on **finish** to proceed to next step.

The screenshot shows the same 'New Case' window, but now the 'Additional Information' tab is active. It contains a message: 'Please enter additional information. This information is not required and can be filled any time through the Properties pane.' Below this, there are several input fields: 'Investigator name:' with a dropdown menu showing 'RAJ CHANDEL'; 'Agency/Company:' with an empty dropdown; 'Phone:' with an empty dropdown; 'Fax:' with an empty dropdown; 'Address:' with a dropdown menu showing 'DELHI'; and 'E-mail:' with a dropdown menu showing 'raj@hackingarticles.in'. There is also a 'Comments:' label followed by a large text area. At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'. A watermark 'www.hackingarticles.in' is visible across the center.

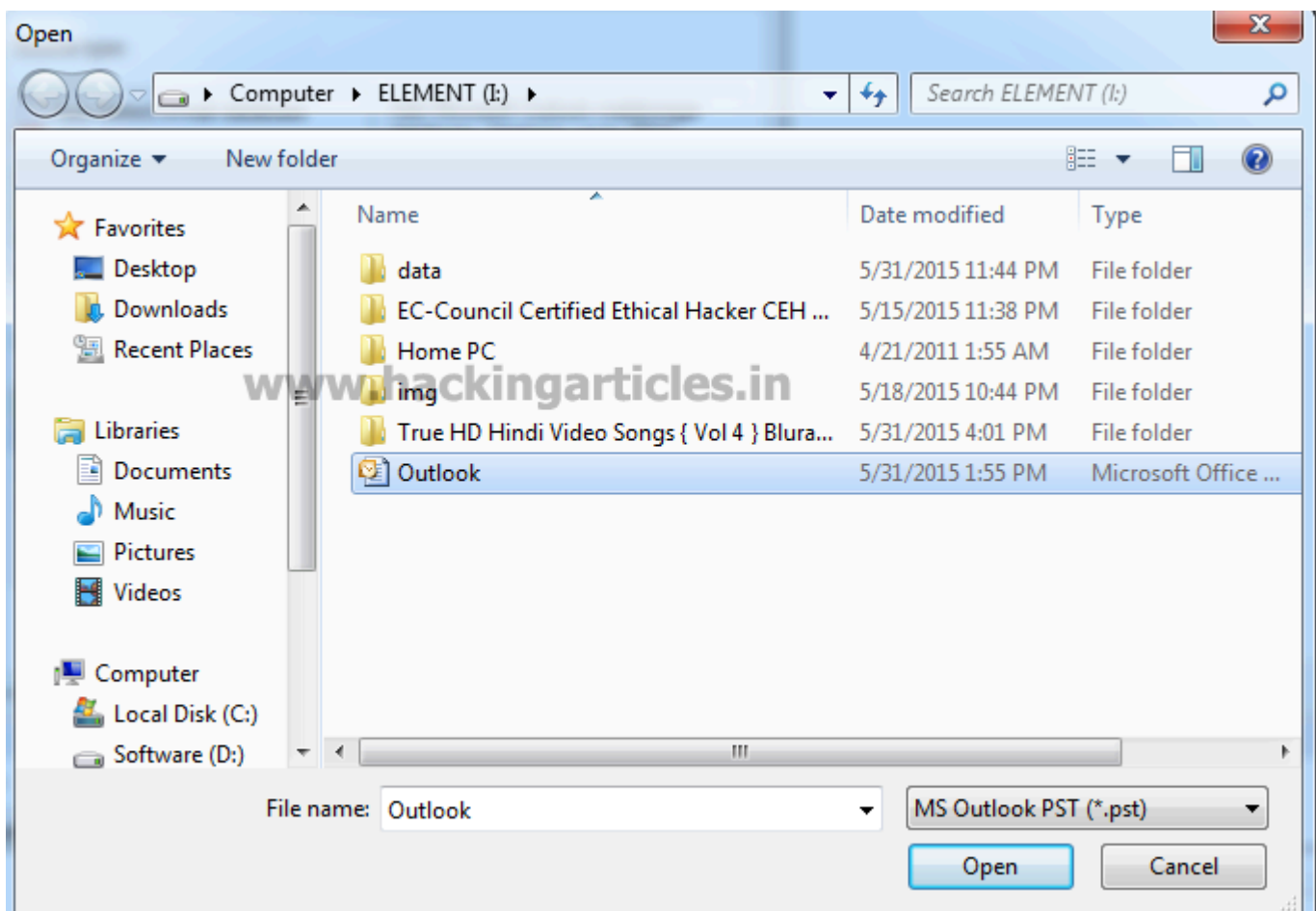
Then it will ask for the file name to save your case in your specified location. Click on save option.



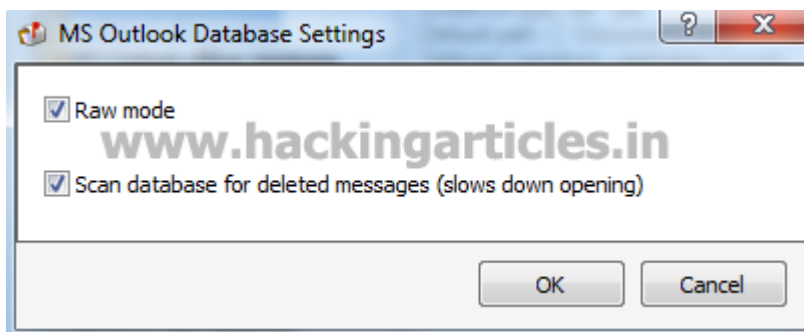
Now select **MS Outlook Image** option from **source type** which will add the outlook image evidence.



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



Now you have to select both option and click on ok to proceed next step.



Now you will see the case **Demo** is created, which will show you the hierarchy of the directories of the evidence outlook image. Now it will allow you to analyze the message header, bodies and attachments.

Paraben's E-mail Examiner Demonstration version - demo.cemx

File View Tools Help

New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History Options

Search Sorting Attachments Sorted Files Search Count Contents Add Bookmark

Case Explorer

Items

- Demo
 - Outlook
 - Outlook Personal Storage
 - Top of Personal Folders
 - Deleted Items
 - Inbox
 - Outbox
 - Sent Items
 - Calendar
 - Contacts
 - Journal
 - Notes
 - Tasks
 - Drafts
 - RSS Feeds
 - Junk E-mail

Properties

General

Inbox

Internal Path: Personal Storage\mbx#000000000000122\mbx#000000000000122:fld#0000000000008022\mbx#0000000000008022:fld#0000000000008082

	Subject	From	To	Created	Sent	Received	Last Modified	Size (bytes)	Info
<input type="checkbox"/>	Re: SSI-Scan "0x3a" <cry	Raj Char		5/29/2015	5/29/2013	5/29/2013 7:51	5/29/2015 7:38:35 PM	15,883	
<input type="checkbox"/>	SSI-Scan "0x3a" <cry	raj@hac		5/29/2015	5/28/2013	5/28/2013 9:01	5/29/2015 7:38:33 PM	10,102	
<input type="checkbox"/>	Notification "4shared" <	raj@hac		5/29/2015	11/1/2014	11/1/2014 11:1	5/29/2015 8:11:54 PM	16,032	
<input type="checkbox"/>	"Aakash Mit	raj@hac		5/29/2015	4/23/2012	4/23/2012 8:26	5/29/2015 7:07:19 PM	10,606	
<input type="checkbox"/>	a friend	"abdel amoc	raj@hac	5/29/2015	8/18/2012	8/18/2012 9:56	5/29/2015 7:12:13 PM	5,435	
<input type="checkbox"/>	"Abdul Sala	raj@hac		5/29/2015	5/21/2015	5/21/2015 1:10	5/29/2015 8:41:18 PM	2,449,736	
<input type="checkbox"/>	Course Fe	"abdul salar	Raj Char	5/29/2015	4/15/2015	4/15/2015 2:21	5/29/2015 8:38:48 PM	22,337	
<input type="checkbox"/>	Fwd: [WA	"abdul salar	Raj Char	5/29/2015	4/10/2015	4/10/2015 6:13	5/29/2015 8:38:46 PM	9,599	
<input type="checkbox"/>	article 1	"abdul salar	Raj Char	5/29/2015	3/28/2015	3/28/2015 11:1	5/29/2015 8:37:53 PM	113,652	
<input type="checkbox"/>	facebook	"abdul salar	Raj Char	5/29/2015	4/24/2015	4/24/2015 4:20	5/29/2015 8:39:06 PM	305,633	
<input type="checkbox"/>	earthinfra	"abdul salar	Raj Char	5/29/2015	3/28/2015	3/28/2015 6:55	5/29/2015 8:37:51 PM	588,053	
<input type="checkbox"/>	Hacking a	"Abdus sala	raj@hac	5/29/2015	10/30/2014	12/5/2014 12:15	5/29/2015 8:11:54 PM	9,121	
<input type="checkbox"/>	Greetings	"Abhi M Bal	raj@hac	5/29/2015	2/13/2013	2/13/2013 9:57	5/29/2015 7:24:46 PM	7,644	
<input type="checkbox"/>	Re: Greeti	"Abhi M Bal	Raj Char	5/29/2015	2/16/2013	2/16/2013 11:1	5/29/2015 7:24:48 PM	20,798	
<input type="checkbox"/>	Re: Greeti	"Abhi M Bal	Raj Char	5/29/2015	2/14/2013	2/14/2013 1:44	5/29/2015 7:24:46 PM	240,191	

Finished Total: 1556

Tasks

Running Completed Queued

Sorting Searching

Name	Source	Destination	State	Progress

Common Log Tasks