eDiscovery Search Inside Gmail Mailbox

Manual & Tool Oriented Strategy Discussed

Web-based email applications such as **Gmail, Yahoo, Hotmail** and many other, have become a global communication services. Gmail is used by vast number of business organizations and personal users because of its secure communication mechanism. However, recently it has been noticed that safety loopholes in emails enables the cyber crooks to perform their illegitimate activities like *spamming, harassment, cyber stalking*, etc.

This whitepaper posits a schema for investigators to perform the in-depth analysis on email artifacts. In particular, it focuses on the various manual and forensic tool oriented methodology to extract evidence from criminals' mailbox. The paper will describe the difficulties faced by experts during examination of Gmail emails along with their possible solutions.

This whitepaper aids the users to:

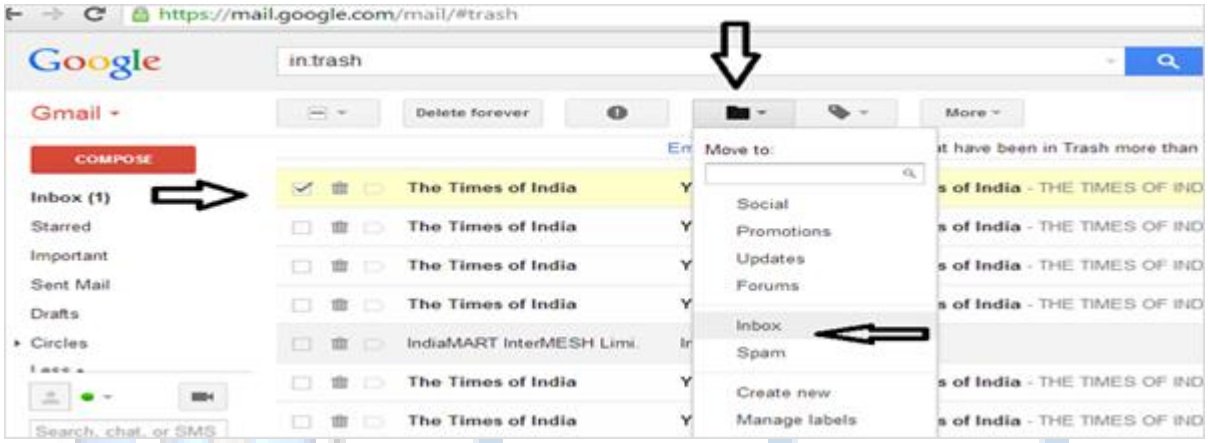
- *Recover Gmail's lost data such as email messages, contact, calendar.*
- *Restore Gmail account.*
- *Deeply analyze the Gmail account via MailXaminer.*

Recover Deleted Gmail Email Messages

After committing the crime, if a culprit does not perform the hard-deletion on email messages, then it can be recovered from Trash folder. Gmail provides the option to restore the deleted emails within 30 days.

User need to follow these steps to back the emails in inbox folder:

- *Sign into Gmail account > Trash >Select the messages > Move to Inbox.*



Google Apps also provide manual procedures to restore the permanently deleted data too, but with some limitations:

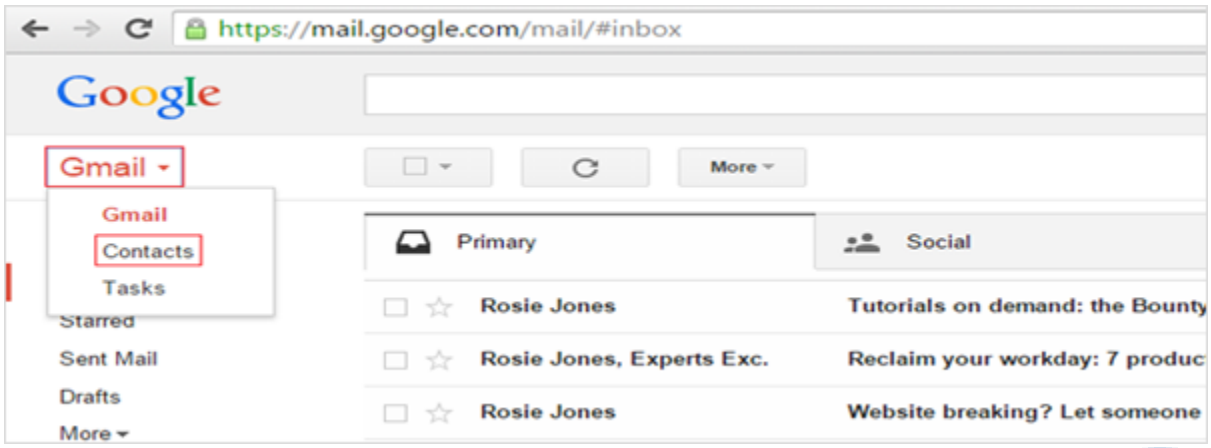
- Admin of the users' account can restore the permanently deleted data but with restriction of only up to 25 days. There is no option to view or select the particular file to restore; admin has only one option either recover all or nothing. Unfortunately, user cannot restore the data on their own; they need to contact their administrator for assistance.

- Another option is **Google Apps Vault**, but it works on only current file versions. The only way to restore the data via vault is to first export it and then import it back manually with the help of administrator.

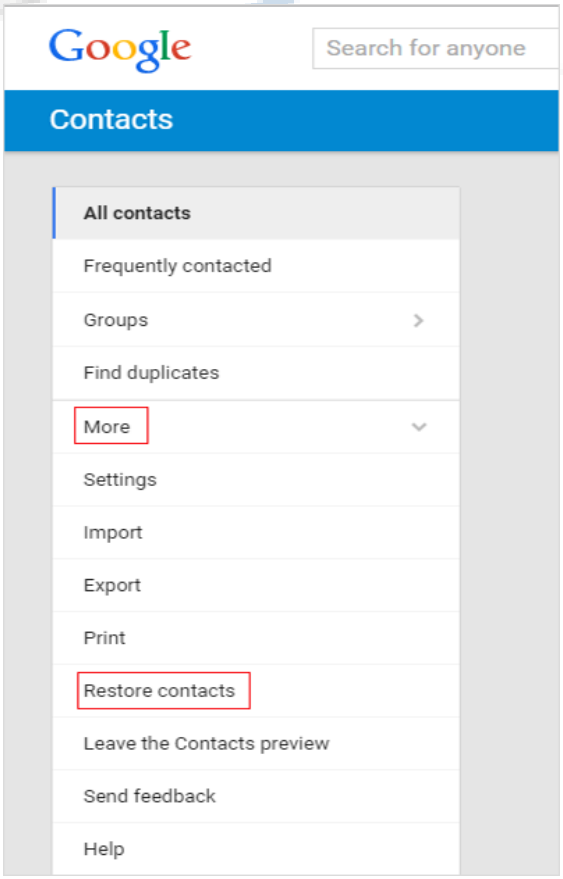
Restore Deleted Gmail Contacts and Calendars

Gmail analysis begins from the offenders' mailbox which contains email messages, contacts, calendar, etc. Gmail has a built-in option to recover objects of contact.

Firstly, click on **Gmail**, then select **Contacts** from the drop down menu.



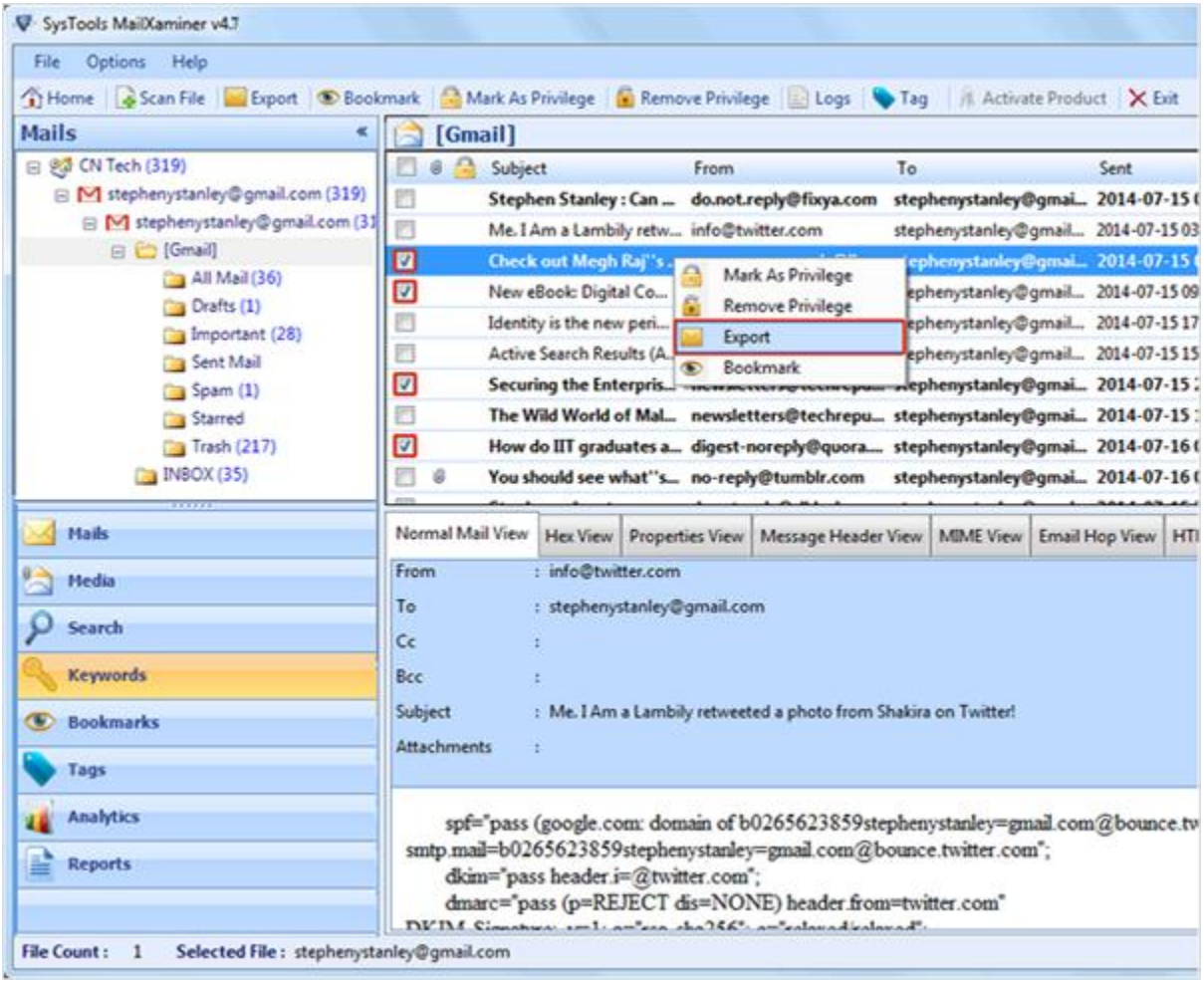
Now, in next pop up window, click on the **More** options and then select **Restore Contacts** from the dropdown menu.



During investigation, techies can use this option to restore the contacts, but it has a limitation that it can recover the data of last 30 days only. To overcome this, experts need a forensic tool like MailXaminer to dig out all evidence from mailbox.

Restore & Analyze Deleted Mailbox Items Using MailXaminer

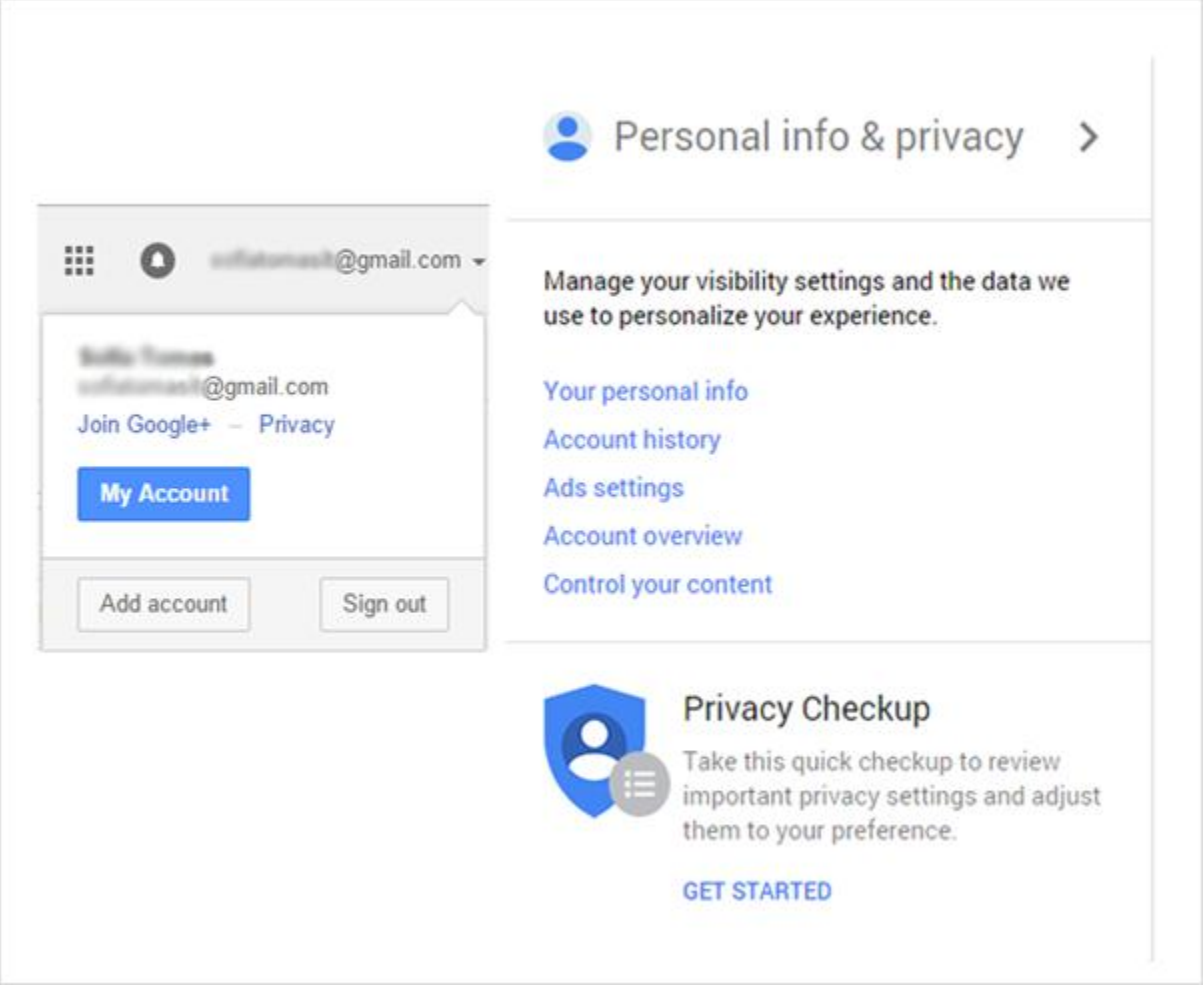
Cybercriminals spoof email messages to carry out various illicit deeds and remain underground to evade any possible legitimate action against them. The one stop solution is MailXaminer. The software consist of the homogenous features that assist the investigators to extract evidence from every angle of Gmail account. The tool enables the experts to view the suspects' email messages into multiple view modes such as *Hex View, MIMIE View, RTF View* and many more. It also provides the **Export** option to extract the artifacts into desired format.



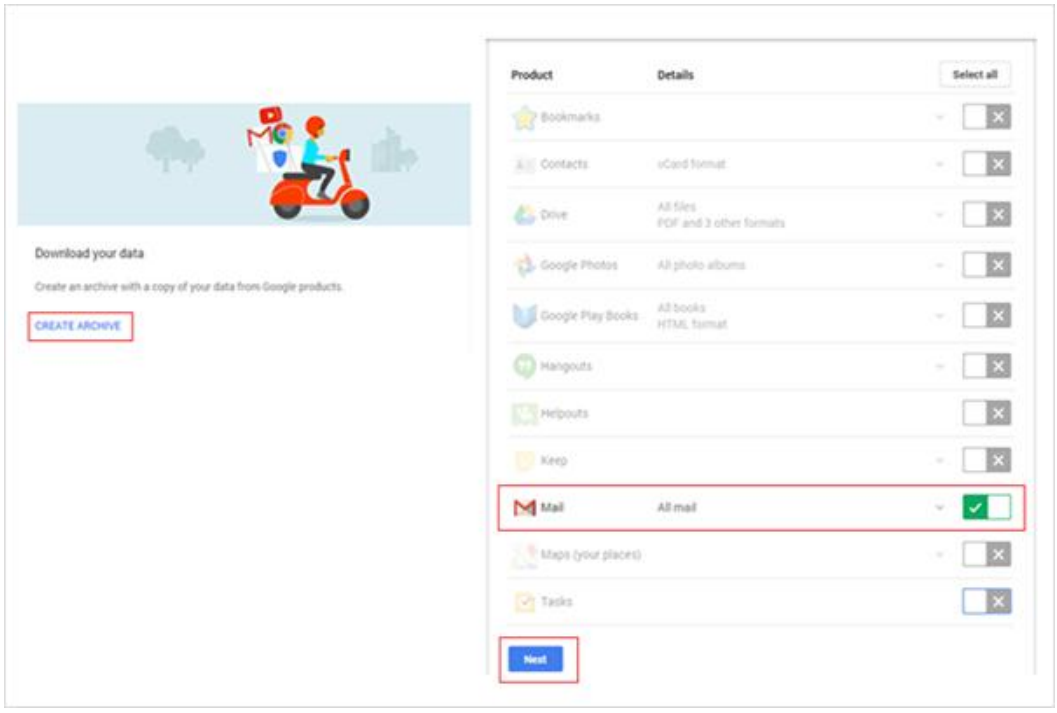
Create Gmail Account Backup via Google Takeout Service

Sometimes investigators need to archive the Gmail account and by using **Google Takeout service**, they can create a backup of culprits' mailbox in a .Zip format.

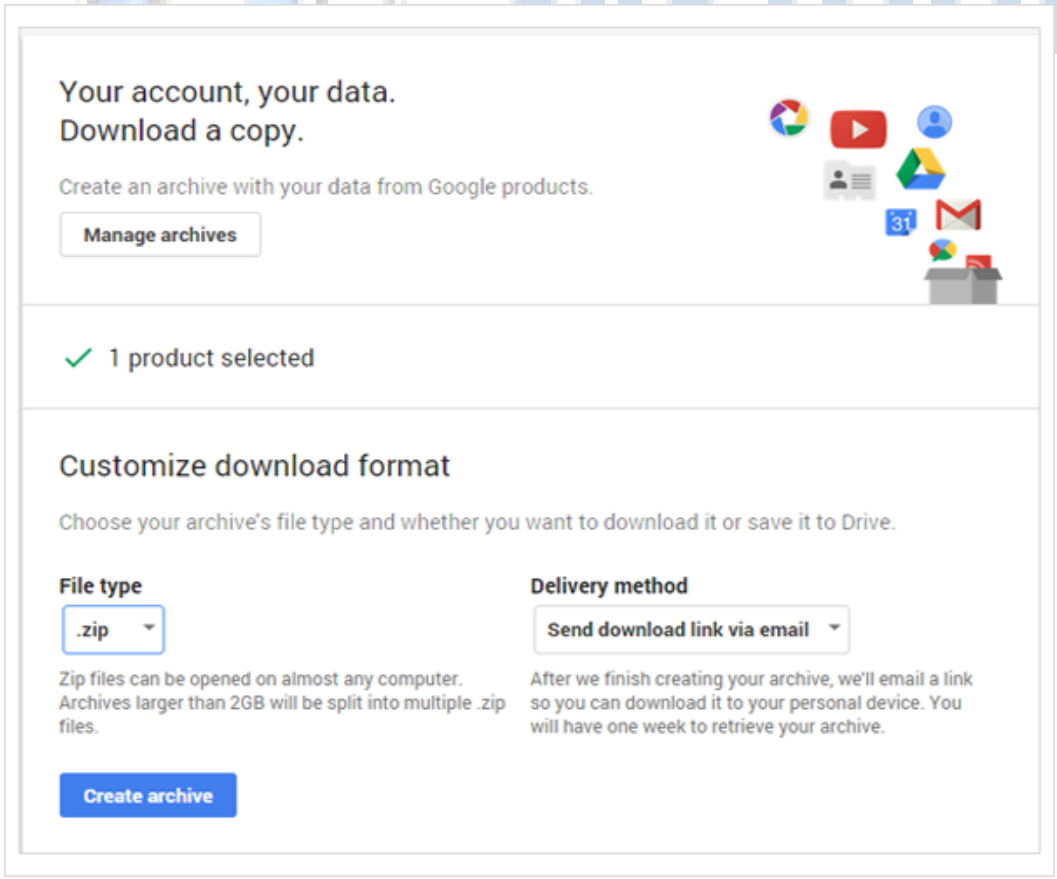
To backup data, click on **My Account** and then click on **Control your content** mentioned under the **Personal info and privacy**.



The next pop-up window shows the option of **Download** your data now, click on **Create Archive** button. On the next page, techies see all the service provide by Google account, check the **Gmail** in the list and click Next.

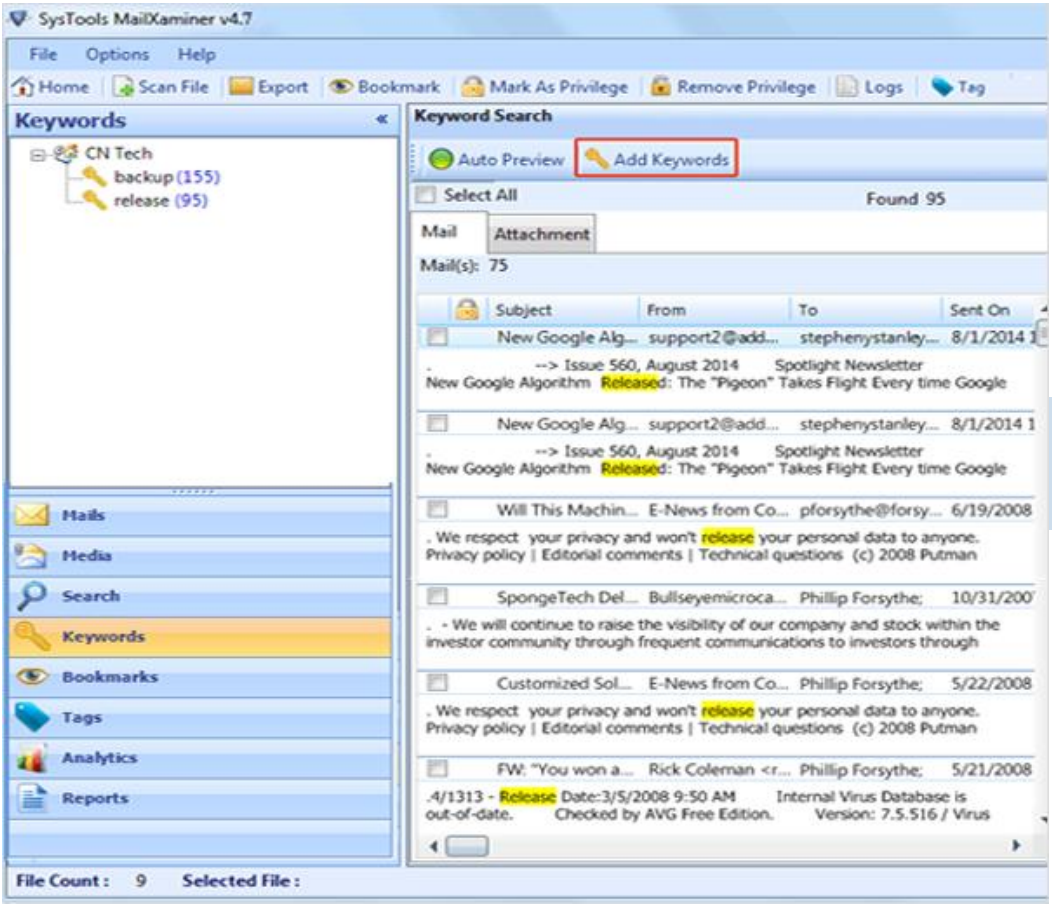


Experts can select the File Type to create backup in desired file format and then click Create archive. After creating the backup and extract the file; user will see **MBOX** file inside it that contains all email artifacts.



Create Backup & Perform eDiscovery Search in Gmail via MailXaminer

Gmail client provides the built-in option to create a backup of users' account but creates a MBOX file that cannot be open by Gmail. Using the software, the techies can easily scan and analyze the email artifacts stored within a MBOX file. Header of any email client contains the most crucial information associated to a criminal email message. The tool assists in examining and sculpting the evidences from header such as *Delivered To, Message ID, Received-SPF* and many more.



One of the most corking features of the software is **Search** option. A search filter enables the experts to search inside the Gmail mailbox via multiple procedures like: *General Search, PreDefined Search, Advance Search, Proximity Search*. With the plethora of features such as *link analysis, skin tone analysis, tagging, multiple export options*, etc., the software is the prime choice of the techies. Our aim is to provide a systematic methodology to perform an efficient examination and forensic investigation on offenders' Gmail account.

Learn step by step instructions to perform **Search** operation and extract evidence from Gmail accounts by following the below mentioned link:

http://www.mailxaminer.com/blog/search-in-gmail/