Uncover Hidden And Lost Email Evidence

Manual & Tool Oriented Strategy Discussed

A number of mechanisms have evolved that help the cyber crooks and corporate guys to conceal, hide and remove the available email data from their respective platforms.

Using this whitepaper, we will be demonstrating various manual and tool oriented techniques to dig into various emailing platforms and carve out required evidences. The tips, techniques and mechanisms are very much confined to the post – investigative strategy where the main purpose of carving out evidence is to support the proceedings running inside the courtroom.

We will demonstrate in detail the procedure to recover and examine the deleted or hidden email artifacts in various platforms such as Microsoft Outlook, Lotus Notes, Gmail, Hotmail, Microsoft Exchange Server, Office 365 and many more.

After reading this whitepaper, you will be able to: -

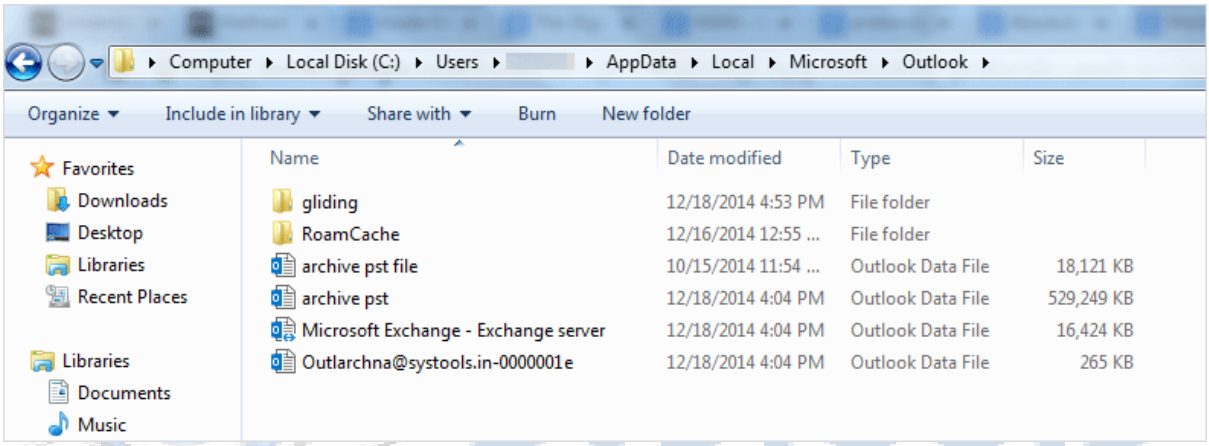
- *Implement available manual methods to recover deleted emails from various respective platforms.*
- *Use the in – built features of emailing platforms to carve necessary evidence.*
- *Use MailXaminer efficiently as a smart approach in digging out the hidden evidence from emails.*

Restore Deleted Items in Microsoft Outlook 2013

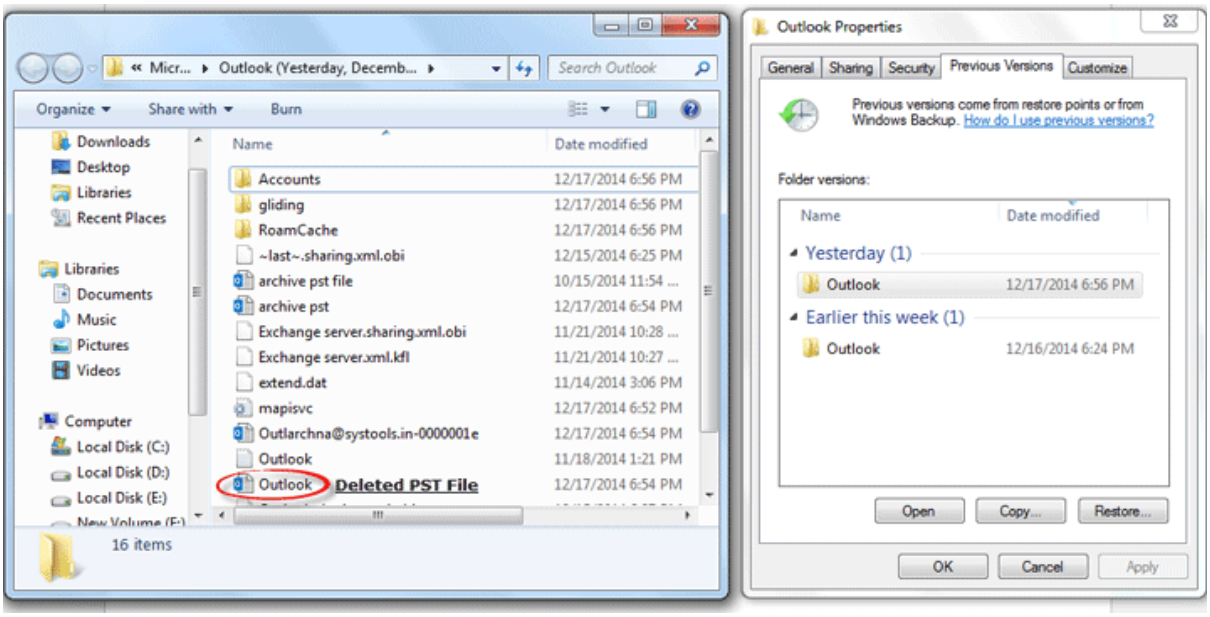
The deleted email items of Outlook 2013 can be recovered on both; Windows 7 as well as Windows 8 operating systems. The only pre – requisite for this manual procedure is that the Outlook email client should be installed on the target machine.

By default, in Windows 7, restore points of the machine are created, thus, creating multiple copies of the stored files and folders. This data can be used to restore the deleted items in Microsoft Outlook 2013.

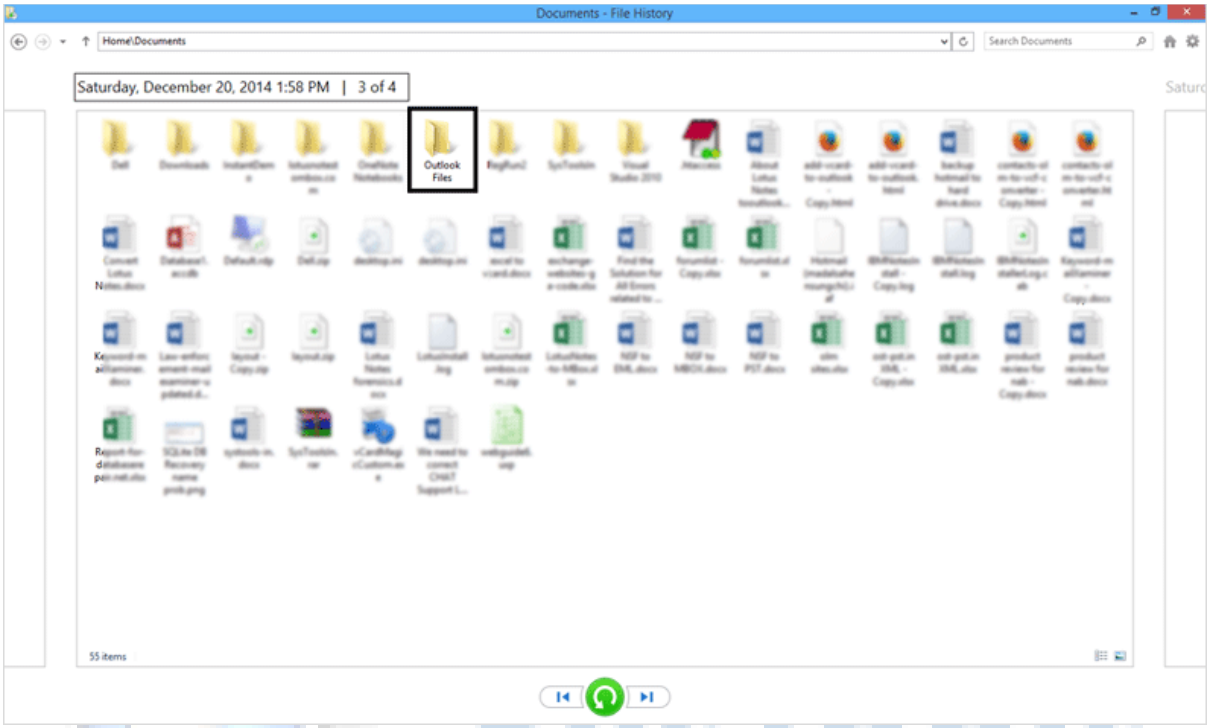
The default location of the Outlook PST file has been shown in the image below: -



Also, you can view the location of PST files in Outlook Folder in the previous versions: -



With the similar approach, in Windows 8 too, the PST files available in the Outlook folder can be recovered from the file history: -



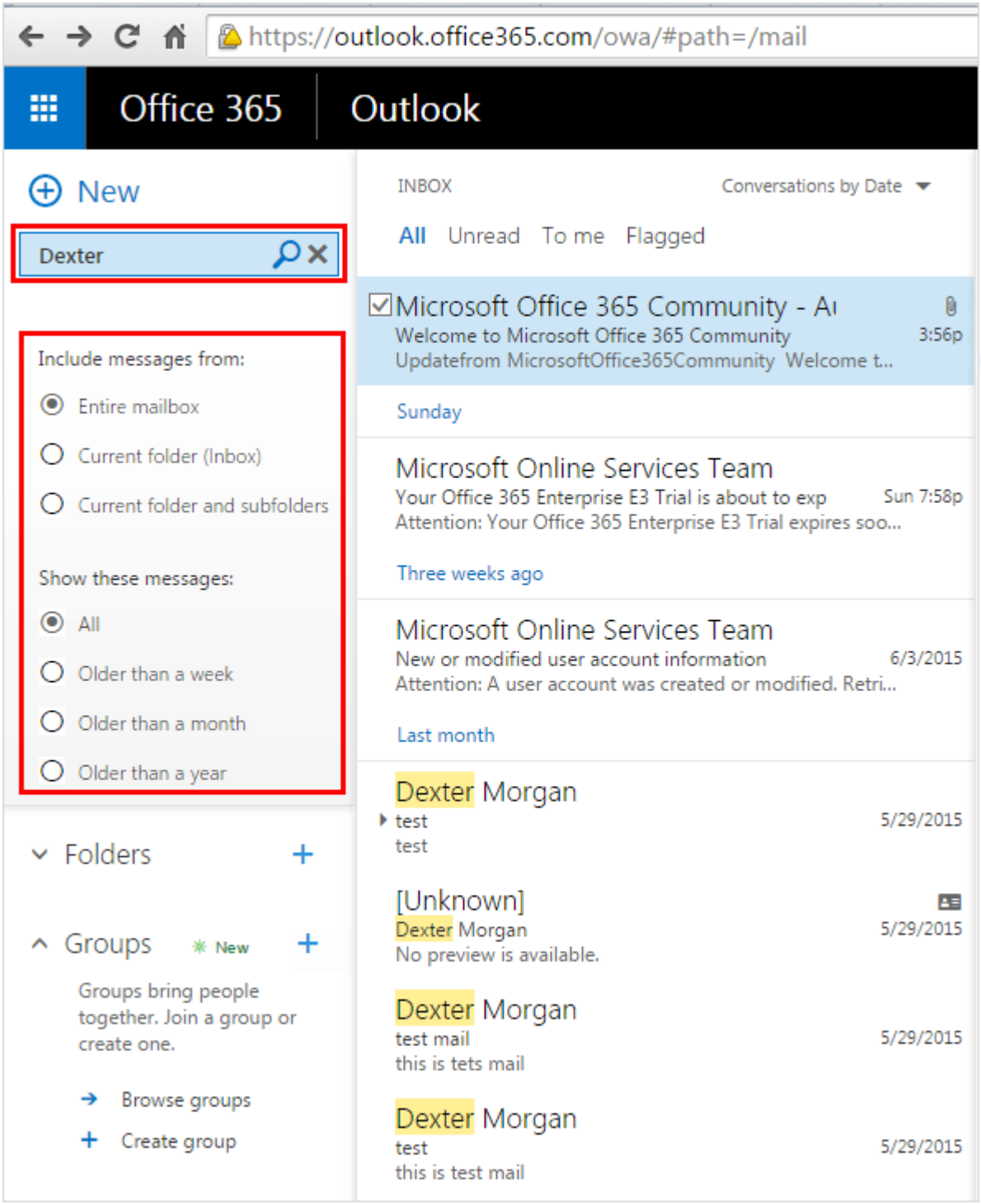
Recover Deleted Items in Outlook PST file using MailXaminer

What if the saving of the previous version files and folders option has not been enabled in Windows 8? What if you need the data available in Outlook folder that was deleted before the creation of restore point?

The solution is MailXaminer. The tool smartly recovers deleted email data from Microsoft Outlook PST files (obviously if the file is not overwritten). Both, the ANSI and Unicode type PST file created in any version of Windows OS can be traversed by the software. MailXaminer does not impose any limitation on the PST file size.

Carry out eDiscovery Search in Office 365 via in – built Search Option

Office 365 offers an inbuilt mechanism for searching the email data available within the mailbox. The search feature provided is very basic and cannot be considered as a smart approach if you are in the need to dig into thousands of emails.



Perform eDiscovery Search in Office 365 using MailXaminer

The various search filters available in the software allow the investigators to search inside Office 365 Outlook mailbox via number algorithms such as usage of logical operators, regular expressions and many more. The search operation is supported by plenty of algorithms in addition to the available email metadata factors such as To, From, Subject and many more.

To learn in detail the complete step by step procedure to perform ediscovery search in Office 365, please visit: -

http://www.mailxaminer.com/blog/ediscovery-search-office-365/

How to Search Evidence in Live Exchange Server without Dismounting The EDB Files?

The scanning of the **Microsoft Exchange Server** mailbox, that too, in live mode without shutting down the Exchange Server is the most typical challenge for the forensic investigators. A slight attempt to dig into the Exchange EDB files in the live mode may lead to crashing down of the Exchange Server, damage or corruption of EDB file, data and capital loss and many more.

MailXaminer smartly allows you to dig inside the live Exchange Server and search for the required email evidences from the EDB file mailbox. The feature is also supported with the feature of **User Impersonation** that allows investigators to dig inside the user mailboxes via transitive relationship.

Follow the detailed steps for Live Exchange Analysis by follwoing the below mentioned link: -

http://www.mailxaminer.com/live-exchange-server-analysis.html

Almost all the email clients leave a trail via which the hidden or deleted email evidences can be recovered but in situations where the detailed in depth analysis with time as well as result based accuracy is in demand, MailXaminer can be taken is consideration.