SIT282/SIT703 Computer Forensics and Investigations

Workshop Session 10

In the previous session, we have learned how to perform advanced encryption and decryption analysis on cases involving multimedia steganography. In this session, we will extract digital evidence from emails. Ubuntu VM is used in this session.

Through this session, you will learn a new tool – readpst for email analysis.

Learning Objectives

1. Perform extraction of digital evidence from emails by applying tools for parsing and analyzing common email file structures.
2. Demonstrate how to perform keyword searches on the extracted email evidence.
3. Interpret findings and write an evidence brief to describe what the results show.

1. Investigating Outlook PST files with readpst

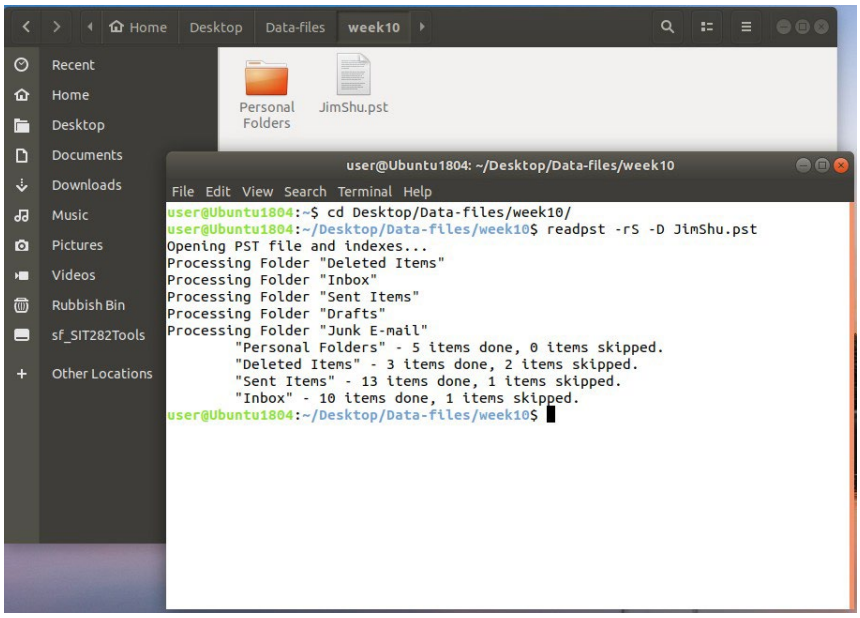
Microsoft Outlook is one of the most popular email client programs. Knowing how to extract information from MS Outlook is important for forensic investigators. Each PST file represents a Message store that contains an arbitrary hierarchy of **Folder objects**, which contains **Message objects** and **Attachment objects**.

Information about Folder objects, Message objects and Attachment objects are stored in properties. The properties collectively contain all of the information about a particular item. To know the insights about PST files and their structures, please refer to the latest Microsoft document. In our case, we will demonstrate Autopsy to parse and analyze email messages inside a PST file.

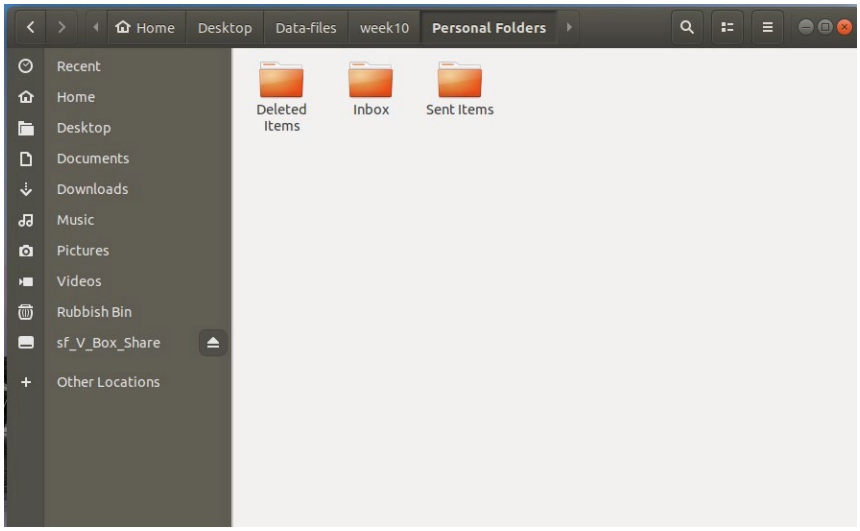
We focus more on the security mechanism of the PST file. According to Microsoft, the PST password can be found as a property value in the Message store and is "a superficial mechanism that requires the client implementation to enforce the stored password". In fact, the password is stored as a CRC-32 hash of the original password string, which is very easy to crack. Hence, anyone can easily read the PST data by cracking this weak password. Thus, the password mechanism for protecting the PST files is not strong and can be broken by using many tools.

Let us show how to investigate a PST file on Linux. Start the virtual machine, and change the directory to "~/Desktop/Data-files/week10". Then launch the readpst program by typing the command "**readpst -rS -D JimShu.pst**". The option "-rS" extracts each item of every folder of the PST file into a separate file, and the option "-D" includes the Deleted items of the PST file. You can read the full description of these options using the "man" command at the prompt i.e. man readpst.

Then a folder named "Personal Folders" will be created according to the contents of the PST file:



You can go through the contents of the “Personal Folders” and find every email and the associated attachments in the folders.



2. Forensic Tasks

Analyze the extracted contents in Section 1. Search for keywords “money” and “cash”, and determine the sender and the receiver. Explore all the hits and the deleted email messages. Can you find a specific image? (Hint: The image relates to tubing material for a bicycle.)

1) Show your results in a readable form to be included in a forensic investigation report.
2) Provide details on how you performed the search including the tools used.
3) Write an evidence brief to describe what the results show.