Case Study

Arrange Evidence Chronologically During Investigation

Prior it could be considered that File Naming Convention is used to make file management easy. However, it has a major role in the Cyber Forensic discipline. Investigators require a broad range of Naming Convention to ensure the digital evidence EMAIL should arrange chronologically in the data storage media and reflect a taxonomy of information. So correct email can be located, identified, and retrieved quickly during the investigation.

This study starts with an overview of one of SysTools client problems related to email cataloging during an investigation and how SysTools Time Based Naming Convention solution helped him. It illustrates the major problems when the appropriate naming conventions of the email files do not take place during a cyber-investigation.

Overview

The use of the descriptive, consistent, and logical naming convention of digital assets promotes consistency and smooth retrieval of data. Comprehensive titling of digital files such as electronic mail plays the utmost crucial role in investigation to comply with legal requirements.

The digital evidence – **EMAIL** is volatile. The unprofessional file nomenclature of this evidence can alter its integrity and makes the electronic mail library chaotic and its retrieval much harder.

One of SysTools clients – Bob, an investigator, faced a cumbersome situation regarding the email file nomenclature during one of its investigations. He ended up with a disaster as he received multiple emails of the same date that was not arranged in chronological order in the storage media. Here SysTools helped him and provided a unique and consistent style of File Naming feature that resolved the Bob problem in an efficacious way.

SysTools®
Simplifying Technology

THE CHALLENGE

A fundamental requirement in digital forensics is to document email files' name in a clear format to maintain their authority and trustworthiness. During an investigation, Bob had to export the email files from the Personal Storage Table [Outlook data file] into PDF format on a designated location. To put all the emails in searchable, single, and chronological order, he saved the email evidence using the naming convention **'YYYY-MM-DD+Subject'.**

However, he found that the multiple emails extracted from a single day are no longer in the chronological format. It was not the correct order. The current naming taxonomy created confusion with other mails and makes it cumbersome to navigate. So whenever he had to find the digital asset quickly he was unable to do so.

Thus Bob decided to change the file's name manually and include the **naming convention** based on the date to make the files in chronological order. However, this operation consumed approximately a week of Bob to modify the name of **2500+ E-mails.**

The only option left for Bob was to use an automatic platform that facilitates a consistent file naming scheme, which would arrange the files in chronological order during the email extraction from PST to PDF on the storage media. It will make the file names more comprehensible and save investigators a ton of work.

SysTools®
Simplifying Technology

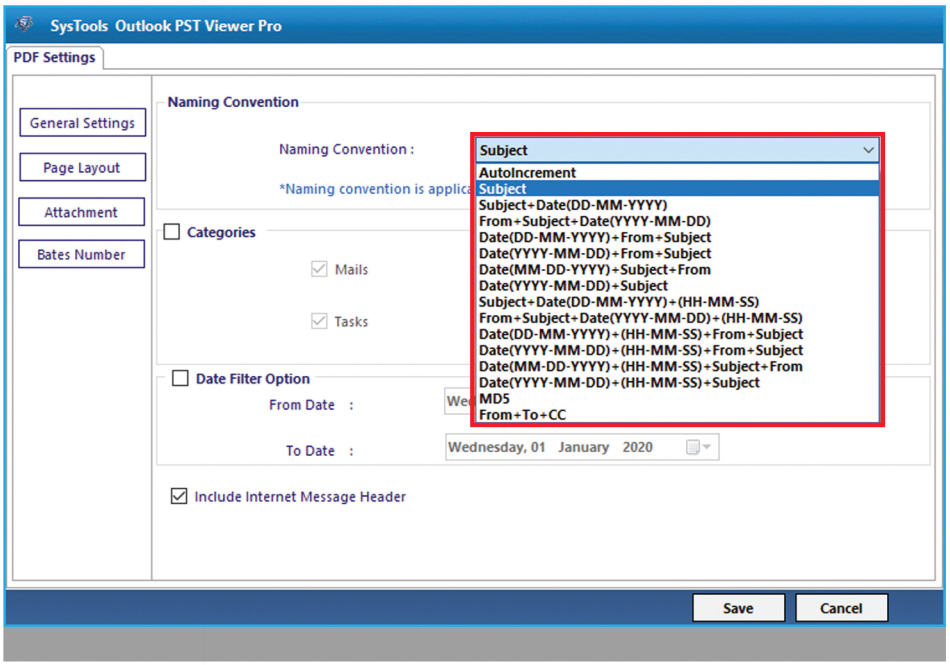
THE SOLUTION

SysTools offered the **Outlook PST Viewer Pro Software** to our client - Bob. The application is engineered to export PST email data to PDF with multiple settings. One of the impeccable features of the wizard is the integration of a wide range of standard file naming convention.

- **Autoincrement**
- **Subject**
- **Subject+Date (DD-MM-YYYY)**
- **Form+Subject+Date (YYYY-MM-DD)**
- **Date (DD-MM-YYYY) + From+ Subject**
- **Date(YYYY-MM-DD) + From+Subject**
- **Date (MM-DD-YYYY)+ Subject+From**
- **Date (YYYY-MM-DD)+ Subject**
- **Subject + Date(DD-MM-YYYY) + (HH-MM-SS)**
- **From+Subject+Date(YYYY-MM-DD)+(HH-MM-SS)**
- **Date (DD-MM-YYYY)+(HH-MM-SS)+From+Subject**
- **Date(YYYY-MM-DD)+(HH-MM-SS)+From+Subject**
- **Date(MM-DD-YYYY)+(HH-MM-SS)+Subject+From**
- **Date(YYYY-MM-DD)+(HH-MM-SS)+Subject**
- **MD5**
- **From+To+CC**

Bob used this solution during the investigation and extracted all the email evidence from the MS Outlook PST to PDF format with convention - Subject + Date (YYYY-MM-DD) + (HH-MM-SS).This time all the resultant emails are saved in Chronological order in the storage media.

This time Bob has files that are well isolated with a descriptive convention. Now it easier for Bob, also fellow researchers, to locate the file without having to click on it and makes the research process more efficient. It enables file accessibility not only by current users but by future users as well.



SysTools®
Simplifying Technology

THE OUTCOME

1. Bob used the PST Viewer application and executed the two operations of his investigation.

- Email Extraction from PST to PDF file

- Saved email evidence in the chrono logical order of the same day via Naming Convention - **Subject + Date (YYYY-MM-DD) + (HH-MM-SS)**

- Saved email attachment file(s) in the chronological order using **FileName or Subject+FileName** in the storage media

2. The solution reduces the investigator's time by automating the email naming convention task and email conversion.

3. A complete return on investment to the client.

4. Eliminates the variability and inconsistencies of emails order processed on the same date that leads to confusion and loss of time during cyber-investigation.

Contact :

SysTools Inc.

**P.O. Box 36, Springville,
Utah - 84663, USA**

**Ph : +1-888-900-4529
www.systoolsgroup.com**

SysTools®
Simplifying Technology