

PFIC



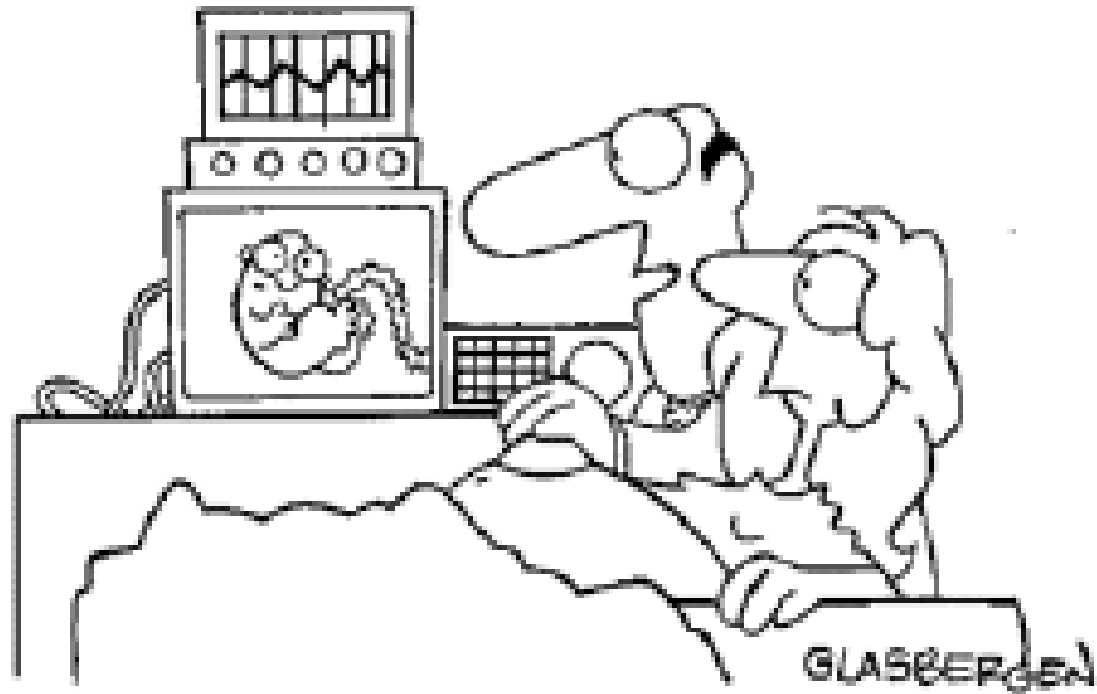
Paraben's Forensic Innovations Conference

Park City, Utah

November 8th-11th 2009

Email Forensics Lab

Using P2 Commander & Network Email Examiner



**“Your baby is developing very nicely.
Would you like to send him an e-mail?”**

What is a local storage archive?



Local storage archives are any archive that has independent archive format from a mail server. Examples of these types of archives include: .PST, .MBX, .DBX, etc.

Basic Rules & Expectations for Local Archives



- 1. Search for the appropriate mail archives and associated data storage.*

Common Local Storage Archives



The Bat!

Index: *.tbi

Messages: *.tbb

The Bat! < v1.42

Index: *.tbx

Messages: *.msb

Forte Agent

Index: *.idx

Messages: *.dat

Pegasus

Index: *.pmi

Messages: *.pmm

FoxMail

Index: *.ind

(E-mail Examiner doesn't use this index file)

Messages: *.box

Outlook Express v5/6

Index+Messages: *.dbx or *.MailDB

MS Outlook

Index+Messages: *.pst (by default messages are stored in encrypted format)

Common Local Storage Archives Cont.

Outlook Express v4.x

Index: *.idx

Messages: *.mbx

Eudora

Index: *.toc

Messages: *.mbx

Poco

Index: *.idx

Messages: *.mbx

Netscape v6.x and 7.x, and Mozilla

Index: *.msf

Messages: *

Netscape < v6.x

Index: *.snm

Messages: *. (no extension)

Basic Rules & Expectations for Local Archives



1. Search for the appropriate mail archives and associated data storage.
2. *Process all items with complete structure of:*
 - Header*
 - Body*
 - Attachment**to compute verification through hash value*

Basic Rules & Expectations for Local Archives



1. Search for the appropriate mail archives and associated data storage.
2. *Process all items with complete structure of:*
 - Header*
 - Body*
 - Attachment**to compute verification through hash value*
3. *Watch for virus issues*

What is a server storage archive?



Server storage archives are any archive that has mixed storage for all of the clients that exist on a server. Examples of these types of archives include: MS Exchange (.EDB), Lotus Notes (.NSF), GroupWise (.DB), etc.

MS Exchange PUB.EDB

■ **Public Information Store**

- contains Public Folders
- Public Folders contain information shared amongst the different users.

MS Exchange PRIV.EDB

■ **Private Information Store**

- contains the mailboxes for the server
- keeps information private from other users.

MS Exchange PRIV.EDB

- **Priv.edb:** A rich-text database file containing message headers, message text, and standard attachments.

MS Exchange PRIV.STM

- **Priv.stm:** A streaming internet content file containing audio, video and other media that are formatted as streams of Multipurpose Internet Mail Extensions (MIME) data.

Lotus Notes *.NSF

■ Valuable Evidence:

- Messages
- Attachments
- PIM Oriented Data

Novell GroupWise Post Office Structure

■ Composed of directories which contain:

- Post Office Database (wphost.db)
 - Admin info required to allow users to exchange messages (list of post offices and associated users)
- Message Store
 - User databases (userxxx.db)
 - Message databases (msgnn.db)
 - Attachments directory

PRACTICAL

