ADVANCED COMPUTER FORENSICS

EnCE EnCase Forensics: The Official EnCase Certified Examiner Study Guide

Chapter 10

Advanced EnCase

Email Importance

- Personal and/or Corporate Communications
- Date and Time Stamps
- Names of other individuals or corporate entities
- Attachments

ENCASE Capabilities

- Search and Parse Speciic Email Types:
  - Outlook
  - Outlook Express
  - Lotus Notes
  - Exchange
  - AOL – MBOX
- Track Email threads and conversations
- Records Tab and All Processed Files

PST Files

- From within the evidence
- From separate .pst files “dragged and dropped” into the case
- Utilize the View File Structure option in order to see the Compound Files
  - Not Recommended due to Viewing and Bookmarking issues.

WEBMAIL

- Has Become VERY Secure HAS BECOME VERY SECURE
  - EnCase will only find bits and pieces from old dialog messages
- Utilize File Carver within the Evidence Processor
  - Carve HTML Files
  - Carve Webmail files

EVIDENCE PROCESSOR

- Records Tab RECORDS TAB
  - Email Folder EMAIL FOLDER
  - Blue Hyperlinked Emails BLUE HYPERLINKED EMAILS
    - Click to View CLICK TO VIEW
    - Launches in a separate window WILL LAUNCH A SEPARATE WINDOW
    - Displays in the Report Tab in the Table View with Attachment
      - Right Click Bookmark

DOL Disclaimer and CCBY

This workforce product was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The product was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.