

SysTools mailXaminer

Beginner • One-Day Instructor-Led Course

For more information contact: info@syntricate.com

The SysTools mailXaminer one-day course provides the knowledge and skills necessary to install, configure and effectively use mailXaminer. Participants will use mailXaminer to conduct forensic investigations on desktop based email, web based email, cloud email, and disk image email artifacts.

Prerequisites

This hands-on class is intended for new users, particularly forensic professionals and law enforcement personnel, who use SysTools software to examine, analyze, and classify email.

To obtain the maximum benefit from this course, you should meet the following requirements:

- Able to understand course curriculum presented in English
- Perform basic operations on a personal computer
- Have a basic knowledge of computer forensic investigations and acquisition procedures
- Be familiar with the Microsoft Windows environment

Class Materials and Software

You will receive the associated materials prior to the course.

During this one-day, hands-on course, participants will perform the following tasks:

- Install and configure mailXaminer
- Review how email works and data is moved from point to point. Acquire email for analysis.
- Create a case in mailXaminer
- Use custom processing function during processing
- Recover information from web based email systems
- Recover deleted emails from desktop email programs
- Recover cloud based email accounts
- Use advanced searching to search through a bulk of messages
 - Regular expression based searching
- Use skin tone analysis
- Bookmarking potential evidence
- Detailed reporting

The class includes multiple hands-on labs that allow students to apply what they have learned in the workshop.

(Continued on other side)



SysTools mailXaminer

Beginner • One-Day Instructor-Led Course

For more information contact: info@syntricate.com

(Continued)

Module 1: Introduction

Topics:

- Overview Of Email
- Email Components
- Email Headers
- Email Header Analysis

Lab:

Participants will install the UTK components—FTK, KFF Library, FTK Imager, Registry Viewer, and PRTK

Module 2: mailXaminer

Objectives:

- Mailxaminer Overview
- Supported Email Categories
- Options – Language Settings
- Options – Advanced Settings
- Settings – Service Settings
- Shortcuts

Module 3: Case Management

Objectives:

- Starting a New Case
- Creating a New Case
- Case Settings – Scan Settings
- Case Settings – Image Analysis
- Case Settings – Video Analysis
- Case Settings – Mail Settings
- Adding Evidence
- Save a Case
- Export a Case
- Open a Case
- Case Overview
- Opening Select Evidence Files
- Close a Case
- Delete a Case
- Import a Case

Module 4: Email Analysis

Objectives:

- Case Overview
- Opening Select Evidence Files
- Case Navigation
- Viewing Emails
- Quick Searching
- Viewing Attachments
- General Searching
- Advanced Searching
- Keywords
- Tagging Emails
- Bookmarking
- Reporting

Module 5: Remote Review

Objectives:

- Team Collaboration
- SmartReview

