nuix | Training

SYLLABUS

NUIX WORKSTATION FORENSIC PRACTITIONER WINDOWS TWO DAY INSTRUCTOR LED CLASS

The Nuix Workstation Forensic Practitioner Windows certification class is designed to teach investigators advanced techniques for Windows investigations using Nuix Workstation and third party utilities in the following ways:

- Identify, analyze, and report on common artifacts of user activity on Microsoft Windows systems.
- Examine how Windows stores information in the Windows registry, the recycle bin, recent items, user directories, and system folders in all versions of Windows.
- Include a detailed look at email including how to identify, sort, search, and deduplicate.
- Learn how browsers store history, cookies, and cache files.
- Understand how the operating system uses link files, prefetch files, and metadata that can be forensically useful

Students will be enrolled in the Nuix Workstation Forensic Practitioner Windows exam. Passing of the Nuix Workstation Forensic Practitioner Windows exam is a requisite for the Nuix Forensic Practitioner Master certification.

MODULE 1: COURSE INTRODUCTION & CLASS OVERVIEW

- Class Introductions
- Class Objectives
- Overview of Nuix Technology
- Nuix Support

MODULE 2: METADATA

- Overview of Metadata
- Metadata Types in Nuix Workstation
- Filter and Search Metadata
- Date and Time Metadata
    - Communication Date
    - Source Time Zone
- Image Metadata
- MS and Open Office Document Metadata
- Derived Metadata Fields
- Custom Metadata Fields

MODULE 3: FILE & SECURITY SYSTEMS

- Disks, Partitions & File Systems
- The Baseline PC Boot Process
- Reparse Points & Symbolic Links
- Windows File System & Partition Structure
- Windows Security & Identify Foundations

MODULE 4: RECOVERING DATA

- Understanding Data Deletion
- The Recycle Bin
- Unallocated Space
- Slack Space

- Windows 10 Recycle Bin
    - Processing
    - Tagging
    - $I File
- Windows XP Recycle Bin
    - Recycler
    - INFO2 File
- Recovering Unallocated and Slack Space
    - Carve
    - Work with Results
    - Exclusions

MODULE 5: EVENT LOGS

- What are Windows Event Logs and How are They Formatted?
    - Where are They Stored and Backed Up?
    - Windows Event Viewer
- Windows 10 Event Logs
    - Log Types
    - Log Views
    - Using the Event Viewer
    - Using Nuix Workstation
    - Create Metadata Profiles for Review
    - Search and Filter
- Windows XP Event Logs
    - Processing in Nuix Workstation
    - Create Metadata Profiles for Review
    - Search and Filter

MODULE 6: REGISTRY BASICS

- Registry Overview
- Understanding the NT Registry Files
- Understanding Forensic Usefulness of Browser Data
- Processing the Registry
    - Smart Processing
- Reviewing Useful SAM, System & Software Registry Artifacts

MODULE 7: LINK & JUMP FILES

- Overview of Windows Shortcuts
- Link Files & Jump Lists
- Distributed Link Tracking Service
- File System Artifacts
- Processing Link Files in Nuix
- Windows 8 Immersive App Link Files

MODULE 8: EMAILS

- Why is Email Important?
- Email Transport and Structure Standards
- Email Transport Protocol
- Email Store Processing
- Exchange Server Databases
- Online Web Mail
    - Processing Settings
- Filtering Emails
- Metadata Profiles for Emails
- Search and Review Emails
- Email Deduplication
- Cluster Runs
- Export Emails

MODULE 9: BROWSERS

- The Most Popular Browsers
    - IE, Firefox & Chrome
- Examining Cached Data, User Settings & History
- Processing Browser Data in Nuix
- Searching & Filtering Browser Data

MODULE 10: PREFETCH & SUPERFETCH

- Overview of PreFetch and SuperFetch
- Settings & Configuration
- Prefetch Files
- Layout.ini Files
- Examining Specific Event Types

For a complete listing of scheduled courses, please visit: **nuix.com/training**

nuix

Nuix (www.nuix.com) creates innovative software that empowers organizations to simply and quickly find the truth from any data in a digital world. We are a passionate and talented team, delighting our customers with software that transforms data into actionable intelligence and helps them overcome the challenges of litigation, investigation, governance, risk, and compliance.

APAC
Australia: +61 2 8320 9444

EMEA
UK: +44 203 934 1600

NORTH AMERICA
USA: +1 877 470 6849