TWO-DAY INSTRUCTOR LED CLASS

SYLLABUS

Nuix Workstation

FORENSIC PRACTITIONER WINDOWS

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, recycle bin, recent items, user directories and system folders in all versions of Windows.
- 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 Nuix Workstation Forensic Practitioner Master certification.

MODULE 1: COURSE INTRODUCTION AND PRODUCT OVERVIEW

- Class Introductions and Objectives
- Overview of Nuix Products and Certification Pathways
- Nuix Support

MODULE 2: METADATA

- Overview of Metadata: What Is Metadata?
- Why Would You Use Metadata in Your Investigation?
- Metadata Types in Nuix Workstation
- Image-Specific Metadata
- Microsoft and Open Office Document Metadata
- Filtering and Searching Metadata
- Date and Time Metadata
- The Nuix ‘Time Hierarchy’ – Item Date
- Communication Date
- Filesystem and Property Time Zones Are Factored In
- Source Time Zone
- Viewing Metadata Efficiently
- Derived Metadata Fields
- Custom Metadata Template

MODULE 3: FILE AND SECURITY SYSTEMS

- Examining the Filesystem Sets the Stage
- Disks, Partitions, and Filesystems in Windows

- PC Boot Process
- Default Disk Partition Layouts in Windows
- Windows Folder Structures
- Reparse Points
- The Basics of Windows Security
- The Active Directory – Windows Big Brother Is Watching

MODULE 4: RECOVERING DATA

- Understanding Data Deletion
- What Is 'Unallocated Space' and Where Can You Find It?
- There's Also Slack Space
- Windows Recycle Bins
- Recovering Data from Unallocated and Slack Space
- Using Nuix Workstation to Carve Unallocated Space - Visibility

MODULE 5: EVENT LOGS

- Why Do We Need Event Logs?
- Windows 10 (Post-Vista) Logs
- The 6 Main Event Log Types
- Default Log View
- Searching and Filtering with Event Viewer
- Exporting and Importing with Event Viewer
- Processing Event Logs in Nuix Workstation
- Create Metadata Profiles for Review
- Interesting Event IDs
- Windows XP Event Logs

MODULE 6: REGISTRY BASICS

- Forensically Useful Artifacts Found in the Registry
- What Is the Windows Registry?
- Registry Keys in Nuix Workstation
- Processing the Registry
- Filter for Windows Registry Files
- The SAM Hive
- The SOFTWARE Hive
- The SYSTEM Hive
- USB Device Information
- Review USB Information with a Metadata Profile
- The USER Hive

MODULE 7: LINK AND JUMP FILES

- Overview of Windows Link Files (Shortcuts)
- The DLT Service
- Automatically Created Link Files – Recently Used Items
- Jump Lists
- Processing Link Files in Nuix Workstation
- Using a Metadata Profile to List Shortcut Data
- Immersive Application Link Files
- Built-In User Activity Filters: Document Navigator

MODULE 8: BROWSERS

- The Forensic Significance of Browsers
- The Browser Wars
- Chrome
- Firefox
- Internet Explorer
- Processing Browser Information
- Search Using Filters and Entities
- Not All Web Searches Are the Same
- **MODULE 9: PREFETCH AND SUPERFETCH**
- Prefetch and Superfetch Defined
- What Can Prefetch / Superfetch Show Us?
- Prefetch and Superfetch Registry Settings
- Prefetch Files
- Prefetch in Nuix Workstation
- Prefetch File Content
- The Layout.ini File

MODULE 10: VISUALIZING DATA USING CONTEXT

- Context Tab
- Analysis Graph

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

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	**EMEA**	**NORTH AMERICA**
Australia: +61 2 8320 9444	UK: +44 203 934 1600	USA: +1 877 470 6849