SYLLABUS

TWO-DAY INSTRUCTOR LED CLASS

Nuix Workstation

FORENSIC PRACTITIONER WINDOWS

The Nuix Workstation Forensic Practitioner Windows certification course 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?
- Metadata Types
- Structural Metadata
- Searching and Filtering Using Metadata
- Date and Time Metadata
- Metadata Profiles: Viewing Metadata Efficiently
- Metadata Types in Nuix Workstation

MODULE 3: FILE AND SECURITY SYSTEMS

- Examining the File System Sets the Stage
- Disks, Partitions, and File Systems in Windows
- Default Disk Partition Layouts in Windows
- Windows 10 Folder Structures
- The Reality of the Master File Table
- System Volume Information
- Windows 7 Folder Structure
- Windows XP Folder Structure
- Windows 10 User Folder Structure
- Windows XP User Folder Structure
- Reparse Points
- The Basics of Windows Security
- What’s in a SID?
- Local Security
- Access Controls (ACLs): The Power to Access Objects
- User Rights – The Power to Take Action
- Active Directory: Windows’ Big Brother Is Watching

MODULE 4: RECOVERING DATA

- What Are We Hoping to Find?
- Understanding Data Deletion
- What and Where Is Unallocated Space?
- There Is Also Slack Space
- Slack Space and NTFS
- Windows 10 Recycle Bin Basics
- The Windows 10 Recycle Bin
- Processing Windows 10 Recycle Bins
- What’s in the $I File?

- Tagging Entries in the Recycle Bin
- Windows XP Recycle Bin
- Windows XP INFO2 File
- Recovering Data from Unallocated and Slack Space
- Using Nuix Workstation to Carve Unallocated Space – Visibility
- Processing Settings for Carving Enumeration
- Reviewing Carving – Enumeration
- Carving with Nuix Workstation: Exclusions
- Caring with Nuix Workstation: Viewing

MODULE 5: EVENT LOGS

- What Are Windows Event Logs and How Are They Formatted?
- Windows 10 Event Logs
- Windows XP Event Logs

MODULE 6: REGISTRY BASICS

- Forensically Useful Artifacts Found in the Windows Registry
- What Is the Windows Registry?
- Processing the Windows Registry
- Filter for Windows Registry Files: Filtered Items
- The SAM Hive
- The Software Hive
- The System Hive
- The User Hive: NTUSER.dat

MODULE 7: LINK AND JUMP FILES

- Overview of Windows Links and Shortcuts
- Windows 10 Immersive Shell Link Files
- Most Recently Used Lists
- Jump Lists
- Processing Link Files in Nuix Workstation
- Windows Immersive Application Link Files
- Built-In User Activity Filters: Document Navigator

MODULE 8: BROWSERS

- The Main Browsers (IE, Firefox, and Chrome)
- Examining Cached Data, User Settings, and History
- Processing Browser Data in Nuix Workstation
- Searching and Filtering Browser Data

MODULE 9: PREFETCH AND SUPERFETCH

- Overview of Prefetch and Superfetch
- Settings and Configurations
- Prefetch Files
- 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