



# 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, 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
- 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
- Windows XP Recycle Bin
- Recovering Unallocated and Slack Space

### **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**

- Registry Overview
- Understanding the NT Registry Files
- Understanding Forensic Usefulness of Browser Data
- Processing the Registry
- 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: BROWSERS**

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

### **MODULE 9: PREFETCH & SUPERFETCH**

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

### **MODULE 10: VISUALIZING DATA USING CONTEXT**

- Context Tab
- Analysis Graph

For a complete listing of scheduled courses, please visit [nuix.com/training](https://nuix.com/training).

---

**nuix**

Nuix ([www.nuix.com](http://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

Nuix (and any other Nuix trademarks used) are trademarks of Nuix Ltd. and/or its subsidiaries, as applicable. All other brand and product names are trademarks of their respective holders. Any use of Nuix trademarks requires prior written approval from the Nuix Legal Department. The Nuix Legal Department can be reached by e-mail at [Legal@nuix.com](mailto:Legal@nuix.com). THIS MATERIAL IS COMPRISED OF INTELLECTUAL PROPERTY OWNED BY NUIX LTD. AND ITS SUBSIDIARIES ("NUIX"), INCLUDING COPYRIGHTABLE SUBJECT MATTER THAT HAS BEEN NOTICED AS SUCH AND/OR REGISTERED WITH THE UNITED STATES COPYRIGHT OFFICE. ANY REPRODUCTION, DISTRIBUTION, TRANSMISSION, ADAPTATION, PUBLIC DISPLAY OR PUBLIC PERFORMANCE OF THE INTELLECTUAL PROPERTY (OTHER THAN FOR PREAPPROVED INTERNAL PURPOSES) REQUIRES PRIOR WRITTEN APPROVAL FROM NUIX.