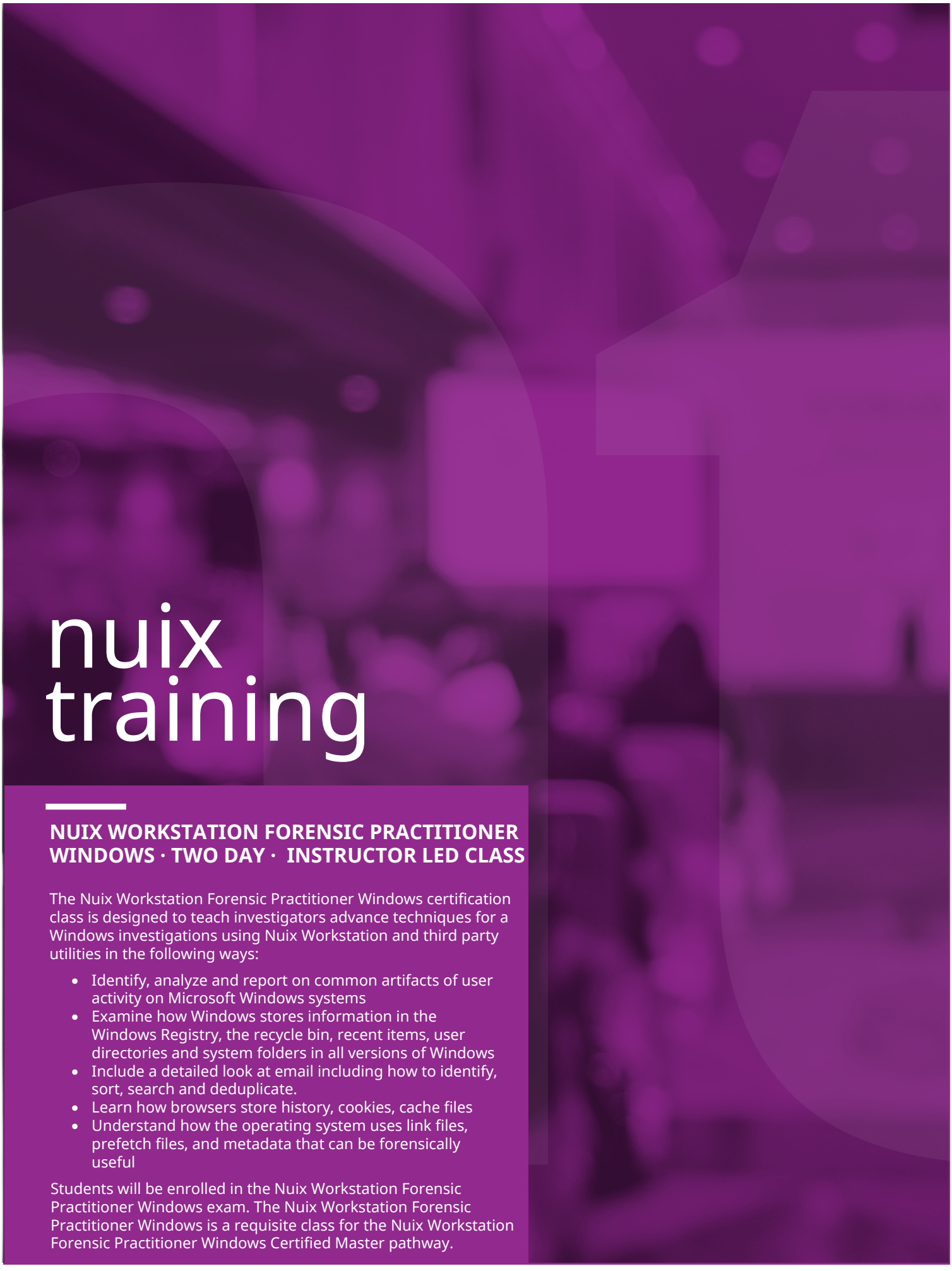

nuix training

NUIX WORKSTATION FORENSIC PRACTITIONER WINDOWS · TWO DAY · INSTRUCTOR LED CLASS

The Nuix Workstation Forensic Practitioner Windows certification class is designed to teach investigators advance techniques for a 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, 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. The Nuix Workstation Forensic Practitioner Windows is a requisite class for the Nuix Workstation Forensic Practitioner Windows Certified Master pathway.

MODULE 1: INTRODUCTION & CLASS OVERVIEW

- Class introductions
- Class objectives
- Nuix history
- Overview of Nuix technology
- Nuix support

MODULE 2: METADATA

- Metadata overview
- File system and MS Word metadata
- Image EXIF data
- Searching metadata in Nuix

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

- Unallocated & Slack space
- Windows Recycle bin
- Data recovery
- Carving with Nuix

MODULE 4: EVENT LOGS

- Windows Event log formats
- Default log views
- Processing logs into Nuix
- Searching and filtering Logs entries

MODULE 5: REGISTRY BASICS

- Registry overview
- Understanding the NT registry files
- Understanding forensic usefulness of browser data
- Processing the registry
    - Smart processing
- Reviewing comply useful SAM, system & software registry artifacts

MODULE 6: 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 7: EMAILS

- Email mailbox processing
- Metadata profiles for email

MODULE 7: EMAILS

- Identifying & handling attachments
- Sorting emails, threads & duplicates
- Cluster Runs
- Email visualizing and reporting

MODULE 8: BROWSERS

- The Main Browsers
    - IE, Firefox & Chrome
- 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

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

nuix

Nuix understands the DNA of data at enormous scale. Our software pinpoints the critical information organizations need to anticipate, detect, and act on risk, compliance, and security threats. **To learn more visit www.nuix.com**.

APAC

Australia: +61 2 8320 9444

EMEA

UK: +44 203 934 1600

NORTH AMERICA

USA: +1 877 470 6849