Nuix Workstation and Windows Artifacts Analysis

The class will lead the user thru the processes of case creation and analysis of various artifacts that can be encountered in the wild, with emphasis on analyzing Windows Artifacts through a Nuix case. We will also discuss and perform workflows intended to improve the overall performance in using Nuix for your investigation needs.

Module 1: Introduction

- Nuix Licensing Types
- The Forensic Process
- System Environment
- Nuix Workstation System Requirements
- Configuration Profiles
- Storage
- Sample Configurations
- Nuix Workstation Installation
- Nuix Imager
- Nuix Support

Module 2: What is Nuix Imager

- What is Nuix Imager?
- Launching the application
- Add Evidence
- Analyzing Artifacts
- Collecting data

Module 3: Processing data in Nuix Workstation

- Nuix Workstation
- Initial Data Processing
- Adding Case Evidence
- Evidence Processing Profiles

Module 4: INTERFACE, FILTERS, AND BASIC SEARCHING

- Nuix Workstation Overview
- View Options
- Document Navigator
- Results Pane
- Results Pane Tabs
- Review Pane

Module 5: 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 6: POST-PROCESSING ANALYSIS
- Forensics: Hiding the Irrelevant
- Start with Statistics
- Irregular Items
- Checking Items: Perform Operations on Items
- Immaterial Items
- Metadata
- Tags
- Review and Tag Pane
- Comments
- Assign Custodian During Processing
- Deduplication (Digests)
- Exclusions

Module 7: SEARCHING ARTIFACTS IN EVIDENCE
- Framing Forensic Searches
- Search Options
- Query Types
- Search Operators
- Filters
- Field Searches
- Save Search
- Search & Tag
- Advanced Search
- Word Lists
- Digest Lists
- Near Duplicates
- Shingle Lists
- Cluster Runs
- Searching Specific MIME Types
- Registry/Database Viewer
- Search Macros
- Pivot
- Charts View

Module 8: NAMED ENTITIES
- Named Entities Overview
- RegEx
- Named Entity Processing Settings
- View Named Entities
- Search Named Entities
- Create Custom Named Entities
- Create Custom Named Entity Profiles

Module 9: ADVANCED FORENSICS AND MOBILE PHONES
- Mobile Phone Analysis

MODULE 10: REPORTING & EXPORTING

- Reporting Basics
- Export Types

Advanced Windows Analysis

Module 1: 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 2: 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 3: EVENT LOGS

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

MODULE 4: 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 5: 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 6: BROWSERS

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

MODULE 7: PREFETCH & SUPERFETCH

- Overview of PreFetch and SuperFetch
- Settings & Configuration

- Prefetch Files
- Layout.ini Files
- Examining Specific Event Types

MODULE 8: VISUALIZING DATA USING CONTEXT

- Context Tab
- Analysis Graph