



Best Practices in Mac Forensics (MFSC-101) 2025 Syllabus

- **Introduction**
 - Sumuri's Mission Statement
 - Instructor's Introduction
 - Traditional Forensic Methodology
 - Differences between Windows and macOS devices
 - Purpose and Scope of Training
 - Class Requirements
 - Student Introductions
- **Apple Device Identification**
 - Desktops
 - Portables (laptops)
 - iPhones
 - Apple Watches
 - Apple TV
 - iPads
 - Apple Vision Pro
- **Apple Technologies**
 - A Brief History of Processors
 - PowerPC
 - Intel
 - Apple Silicon
 - BIOS
 - Open Firmware
 - EFI
 - Apple Silicon Firmware
 - Apple Configurator 2
 - Device Firmware Upgrade (DFU) mode
 - Windows on Mac
 - Bootcamp
 - Intel Macs
 - Virtualization
 - Intel Macs
 - Apple Silicon Macs





- **macOS Overview**
 - Classic Mac OS
 - Mac OS X
 - macOS Major Features
 - macOS 12 Monterey
 - macOS 13 Ventura
 - macOS 14 Sonoma
 - macOS 15 Sequoia
- **macOS Terminal**
 - macOS Terminal basics
 - GUI vs Kernel vs Terminal
 - Benefits of using the Terminal
 - Accessing the Terminal
 - Command String
 - Elevating Privileges to Root
 - Helpful hints
 - Common Commands
- **Introduction to the macOS Desktop**
 - Using the Trackpad
 - Gestures
 - Dock
 - Standard vs. User Added Applications
 - Identifying Running Applications
 - Trash
 - Finder
 - What is the Finder
 - Finder Window
 - Review of Finder Toolbar
 - Preferences
 - Volume Icons
 - Sidebar
 - Show Path and Status Bar
 - Apple Menu
 - Apple Menu
 - About This Mac / System Report
 - Recent Items
 - Force Quit
 - Application Menus
 - Status Menu





- Spotlight
 - Control Center
 - Siri
 - Notification Center
- Keyboard shortcuts
- Review of Native macOS Applications
 - Functions of Applications
 - Default “Save To” locations
 - Determining if an Application is Running
 - How to Quit an Application
 - Instructor-Led Hands-On Overview
- **Gathering Intelligence (System Settings introduction)**
 - Overview
 - Apple ID
 - Family Sharing
 - Internet Accounts
 - Users & Groups
 - Security & Privacy
 - Passwords
 - Network
 - Sharing
 - Time Machine
- **macOS Directories**
 - Show Hidden Files
 - Root Directories
 - User Home Directories
 - Role of the User Library
- **Viewing Files Natively**
 - Finder View Options
 - Quick Look
 - Expanding Quick Look Functionality via Plugins
 - Preview App
 - TextEdit
- **Documentation and Reporting**





- Screen Capture Options
- QuickTime Player Screen Recording
- Instructor-Led Reporting Overview (PDF Creation and Editing)
- **macOS Forensic System Setup**
 - Installing Xcode
 - Property List Editor
 - Provides necessary Binaries
 - Python 3
 - FUSE for macOS
 - Paragon Drivers
 - MacPorts
 - Installing DC3DD
 - Brew
 - DB Browser for SQLite
 - File Juicer
 - Easy Find
 - Application Full Disk Access
- **macOS File Systems**
 - Supported Read-Write File Systems
 - macOS Extended
 - APFS
 - ExFAT
 - MS-DOS (FAT)
 - Supported Read-Only File Systems
 - NTFS
 - CDFS / UDF
- **Disks and Volumes**
 - Disk and Volume Nomenclature
 - macOS Extended
 - Real vs. Virtual vs. Synthesized
 - Apple Core Storage
 - Fusion Drives
 - APFS
 - Physical Store Disk
 - Container Disk
 - Synthesized Disks





- Virtual Volumes
- APFS Snapshots
 - System Volume Snapshots
 - Time Machine Snapshots
- **macOS Disk Utility**
 - Introduction
 - File System Initialization Options
 - Journaling
 - Encryption
 - Case-Sensitive
 - Partition Schemes
 - Media Sterilization
- **Data Recovery**
 - TRIM and SSDs vs. Traditional Disks
 - APFS
 - Snapshots
 - Viewing Snapshots in Disk Utility
- **Startup Options**
 - Intel Macs
 - Boot Options (Option Key)
 - Recovery Mode
 - Internet Recovery Mode
 - Single User Mode
 - Target Disk Mode
 - Apple Silicon Macs
 - Boot Options
 - Recovery Mode
 - Share Disk Mode
- **Security**
 - Layers of Protection
 - Hardware
 - Intel Mac
 - T2 Security Chipset
 - Data encrypted at rest





- Secure Boot / Disabling Secure Boot
 - Apple Silicon
 - Secure Storage
 - Secure Boot
 - System Integrity
 - Data Protection
 - Touch ID
 - Software
 - Firmware Password
 - Setting
 - Options to remove
 - Sandboxing
 - Containers
 - Data Partition
 - System Integrity Protection
 - Disabling
 - FileVault 2
 - Keychain
 - User Levels
 - Admin
 - Root
 - Standard
 - Guest
 - Resetting a User Password
 - Methods
 - Issues
- **Collecting Volatile Data**
 - What is Volatile Data
 - Examples
 - Concerns
 - Suggested commands
 - Collecting Volatile Data Safely
 - Shell profile files.
- **Apple Evidence Collection (Best Practices)**
 - Importance of Knowing the Password
 - Isolate - Physically





- Isolate - Remotely
 - Active On and Power Nap
 - Identifying and Killing Destructive Processes
 - Changing Power Settings
 - Check User Status (Admin or Standard User)
 - Hidden Desktops and VMs
 - Mounted and Network Volumes
 - Check For Encryption (Drives and FileVault)
 - Collect Volatile Data
 - Live Imaging for Encrypted Filevault Volumes or Network Drives
 - Time Machine Backups
 - Imaging RAM
 - Shut Down Options
 - Transporting a Live Mac
- **macOS Forensic Imaging**
 - Traditional
 - Logical
 - T2 Chipset
 - Apple Silicon
 - Native vs Reverse Engineering
 - Factors to Consider
 - Live Imaging (Apple Silicon)
 - Native Mac Forensic Image Formats
 - Mounting Native Mac Images
- **Apple Extended Metadata**
 - Types of Metadata
 - The Extended Metadata Process
 - Extended Metadata & Non-Apple File Systems
 - AppleDouble Files
- **macOS Index Searches**
 - Spotlight
 - Indexing
 - Preferences
 - Boolean Operands
 - Filters





- Adding Attributes
 - Metadata Commands
 - Utility
 - List
 - Find
 - Forcing Spotlight Indexing
 - Necessity for Shadow Files with Locked Volumes
 - Modifying Searches
 - Bookmarking and Tagging
 - Smart Folders
-
- **Manually Finding Evidence**
 - User Library
 - Property List Files
 - Types
 - Viewing Data
 - SQLite Files
 - Viewing Data
 - Examining Native macOS Applications
 - Contacts
 - Messages
 - FaceTime
 - Notes
 - Calendar
 - Reminders
 - Safari
 - Photos
 - Mail
 - Maps
-
- **Final Thoughts**
 - Importance of owning a Mac
 - Choosing a Mac for Forensics
 - Supporting Hardware
 - Integrating with Windows-based Labs
 - Benefits of Virtual Machines on Mac
 - File System Requirements
 - Mac Forensics with Native vs Non-Native Tools





- **CFME Process**
 - Overview of the CFME exam process
- **Overview of SUMURI Solutions (Post class/Upon request from Students)**

