Best Practices in Mac Forensics (MFSC-101)
2021 Syllabus

- **Introduction**
  - Traditional Forensics (the old ways)
  - Differences between Windows and Macs
  - Purpose of this Training

- **Apple Device Overview**
  - Desktop
  - Portable
  - iPhones
  - iPads
  - Apple Watch
  - Apple TV
  - Air Tags

- **Apple Technology Overview**
  - 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
      - M1 Silicone Macs

- **History and Major Features of macOS**
  - Classic Mac OS
  - Mac OS X
  - macOS 11
  - macOS 12 (Upon Release)

- **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
      - Recent Items
      - Force Quit
    - Application Menus
    - Status Menu
    - Spotlight
    - Control Center
    - Siri
    - Notification Center
  - Keyboard shortcuts

- **Review of Native Applications**
  - Functions of Applications
  - Default “Save To” locations
  - Determining if an Application is Running

  - How to Quit an Application
  - Instructor Led Hands-On Overview

- **System Preferences**
  - Overview
  - Apple ID
  - Family Sharing
  - Internet Accounts
  - Users & Groups
  - Security & Privacy
  - Network
  - Sharing
  - Time Machine

- **macOS Directories**
  - Show Hidden Files
  - Root Directories
  - User Home Directories

- **Viewing Files Natively**
  - Finder View Options
  - Quick Look
  - Cover Flow
  - Preview App
  - TextEdit

- **Documentation and Reporting**
  - ScreenShots
  - PDF Creation
  - QuickTime Player Screen Recording

- **Setting Up Your Mac for Forensics**
  - Choosing your Mac
  - Installing Xcode
    - Property List Editor
    - Necessary Binaries
  - Python 3
  - FUSE for macOS

- Paragon Drivers
- MacPorts
  - Installation
  - Install Pors
    - DC3DD
- DB Browser for SQLite
- File Juicer
- Easy Find
- Application Full Disk Access

- **macOS Terminal**
  - Why do I need to learn the Terminal?
  - Bash vs. ZSH
  - Command String
  - Elevating Privileges to Root
  - Common Commands
  - Helpful Hints

- **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

- **Introduction to Disk Utility**
  - File System Initialization Options
  - Journaling
  - Encryption
  - Case-Sensitive
  - Partition Schemes
  - Media Sterilization

- **Data Recovery**
  - TRIM and SSDs vs. Traditional Disks
  - HFS+
  - APFS
    - Snapshots
    - Space Manager Queue

- **Startup Options**
  - Intel Macs
    - Boot Options (Option Key)
    - Recovery Mode
    - Internet Recovery Mode
    - Single User Mode
    - Target Disk Mode
  - Silicon Macs
    - Boot Options
    - Recovery Mode
    - Share Disk Mode

- **Security**
    - Levels of Protection
    - Hardware
        - Intel Mac
            - T2 Security Chipset
                - Data encrypted at rest
                - Secure Boot
                - Disabling Secure Boot
            - M1 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
  - Trusted Utilities Disk

- **Mac Search and Seizure 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

- **Forensic Imaging**
  - Traditional
  - Logical
    - T2 Chipset
    - M1 Silicon
  - Native vs Reverse Engineering
  - Factors to Consider
  - Image Formats

- **Physical Disk Imaging**
  - Intel
    - Target Disk Mode
  - M1 Silicon
    - Sharing Mode

- **Mounting Images in a Mac**

- **Apple Extended Metadata**
  - Types of Metadata
  - The Extended Metadata Process
  - Extended Metadata & Non-Apple File Systems

- **Indexed and Live Data Searches**
  - Apple Extended Metadata
  - Spotlight
  - Content Searches

- **Bookmarking and Tagging**

- **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

- **Trash**

- **Viewing Suspect Files Natively**
  - File Locations
  - Copy Over Procedure
  - Viewing the Data

- **Overview of MFSC-2 Course**

- **Overview of SUMURI Solutions (Post class/Upon request from Students)**