Advanced Practices in Mac Forensics (MFSC-201)
2025 Syllabus

- **Introduction**
  - Sumuri's Mission Statement
  - Instructor's Introduction
  - Review of MFSC-101 Course
  - Purpose of MFSC-201 Training
  - Helpful Hints
    - Showing Hidden Files
    - Elevating your Privileges to Root in Terminal
    - Xcode Installation

- **Advanced File System Artifacts**
  - Domains
    - System
    - Local
    - User
  - Property Lists
    - Standard
    - Binary
  - SQLite Database Files
  - Bundle Files
  - Library Directories
    - Purpose of Common Directories
      - Application Support
      - Caches
      - Containers
      - Preferences
    - System Domain Library
    - Local Domain Library
    - User Domain Library
  - Finding Artifacts
    - User Account Creation
    - Guest User Account Status

        - Last Logged On User
        - Deleted User Accounts
        - Printer Artifacts
        - Finding Attached Devices
        - Computer Name
        - Finding Network Connections
        - Finding Network Connected Devices
        - macOS version
        - Connected Devices
        - MAC Address
        - Determine Mac Model Type
        - Identify Mounted Volumes
        - Hibernation Status for Building Timelines

- **macOS Alias Files, Hard Links & Symbolic Links**
    - When & How Used
    - Types
        - Alias
        - Hard Links
        - Symbolic Links

- **Mac Timestamps**
    - POSIX
    - Apple Extended Attributes

- **Log Analysis**
    - User Domain Logs
    - Local Domain Logs
    - System Domain Logs
        - Unified Logs
            - Collecting Unified Logs
    - Console Viewer
    - Practical Exercise - Finding Log Artifacts
        - Finding System Startup Times
        - Finding User Logins
            - Success
            - Failed Attempts

        - Remote Login and Sharing
            - SSH
            - Screen Sharing
        - Hibernation Artifacts
        - Wake Reasons
        - Shutdown Times
        - Printer Artifacts
        - Installed Applications
        - iCloud Accounts
        - Starting and Stopping Applications
        - File Access or Opens
        - Finding Attached Devices
        - Finding Network Connections

- **Application Deconstruction – Static Analysis**
    - Artifact Locations
        - User Library
        - Local Library
    - Manual Locating & Analysis of App Artifacts
    - Group Presentations

- **Advanced Command Line for Forensics**
    - Legacy Attributes
        - GetFileInfo command
        - SetFile command
    - Chaining Commands
    - Search Commands
        - Locate command
        - Find command
        - Grep command
    - Searching Logs with Command Line

- **Advanced Search Techniques**
    - EasyFind

- **File System Event Monitoring**
    - ps command

- opensnoop command
- Activity Monitor
  - How to Use
  - Saving Data
- FSEvents Parser

- **Live Log Analysis**
  - macOS System Logs
  - iPhone Live Monitoring

- **Application Deconstruction – Dynamic Analysis**
  - Use of Automated Searching
  - Additional Artifact Locations
  - Analysis of Additional Artifacts
  - Group Presentations

- **Document Versions**

- **Time Machine Forensics**
  - Local Time Machine Snapshots
  - Time Machine Artifiacts

- **RAM Analysis**
  - Current Issues in RAM Capture
  - Creating a RAM Image
  - Data Carving
  - Volatility

- **Virtual Machines Forensics**
  - VM Artifacts
  - VM Best Practices
  - Converting Images

- **iOS Artifacts on Mac**

- **iCloud and Continuity Artifacts**

- **Apple RAIDs**
  - Types of RAIDs
  - Detecting RAIDs

- **Password Recovery**
  - John the Ripper
  - DaveGrohl
- **AppleScript and Automator for Forensics**
  - How to Use
  - Practicals

- **Building Your Own Tools Module**
  - Introduce basic scripting and SQL queries.
    - Tool 1 - Mounting an Image
    - Tool 2 - Volatile Data Collection Script in Bash
    - Tool 3 - Triage Script in Bash/Python

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