Ducara Info Solutions (P) Ltd.

C|MFX

Certified Mobile Forensics Expert

www.ducarainfo.com

WHY C|MFX?

Earn expertise skills in Securing Mobile-based Applications.

- This C|MFX course is designed to allow the student to not only learn but have hands-on experience in examining mobile devices with tools.
- Students will get an understanding of **iOS** and **Android** devices.
- This course is also designed for students to understand the architecture, file system, and appropriate tools for analysis.

UCARA

Are you in Trends?

- The adoption of mobile devices has drastically changed the mobile forensics industry in just the **last year** alone, and the evolving landscape presents newer challenges that demand investigators to rethink the way they work.

    - Forensics experts reveal that multiple **Devices**, **Field Analysis**, **Social Evidence**, **Big Data** and **Mobile Malware** will be the driving factors in shaping the industry this year.

What is the Objective?

Outcome Of this Course

- This course is designed for **Forensic Investigation Professionals** and deals with **Mobile Forensics**.
- The course assumes a prerequisite knowledge of computer security and digital data structures as well as the legal aspects of admissibility of evidence in court.
- It covers the essentials of **Mobile File Structures**, **Data Extraction**, **Analysis** and **Reporting**.
- This course will teach investigators the tools and techniques to perform **Mobile Data Extraction**, **Mobile Data Analysis** and **Evidence Reporting** on different mobile devices.

Target Audience

Who earns C|MFX?

- Forensic Examiner
- Digital Media Forensic Analyst
- Evidence/ Forensic Lab Manager
- Computer Forensics Analyst Lead
- Mobile Device Forensics Specialist
- Incident Management/ IR Consultant

Duration: 32Hrs

TOPICS COVERED

Module 1

Overview of Mobile Forensics

- History of mobile phone examinations
- List the types of data you should look for on mobile devices
- List the different software applications used in this course for mobile device examination
- Describe methods of extracting data manually (if no software applications are available)

Module 2

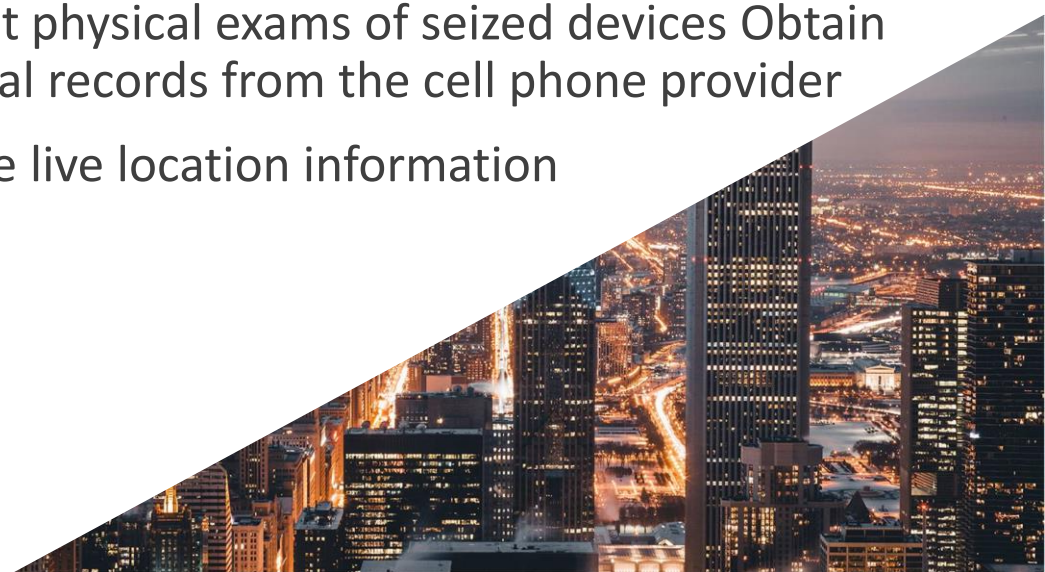
Cellular Networks

- Explain how mobile phones communicate on cellular networks
- Explain how cell sites are configured
- Provide a brief history of mobile network technology(2G, 3G, and 4G)
- Identify the parts of a cellular network

Module 3

Legal Issues

- Provide an overview of case laws that deal with legal issues regarding device and electronic data seizure
- Identify what paperwork is needed
- Conduct physical exams of seized devices Obtain historical records from the cell phone provider
- Retrieve live location information



UCARA

Module 4

Forensic Acquisition of Smartphones

- Logical Acquisition
- File System Acquisition
- Physical Acquisition
- Advanced Methods

UCARA

Module 5

Retrieving User Activity Information from Android Devices

- Android Applications
- Data Structures on Android Smartphones
- SMS / MMS
- Calls, Contacts, and Calendars
- E-mail and Web Browsing
- Location Information
- Third-Party Applications
- Retrieving Deleted SQLite Records
- Retrieving Deleted Data from Raw Images on Android Devices

Module 6:

Android Forensics in Depth

- Android Architecture/Android Components
- NAND Flash Memory in Android Devices
- Android File System Overview
- Android Acquisition Considerations
- Methods Available
- Physical
- File System
- Logical/Backup
- Understanding the Limitations of Extraction Options
- Understanding Traces Left Behind
- Android File System Structures
- Defining Data Structure Layout
- Data Storage Formats
- Parsing and Carving Data
- Physical and Logical Keyword Searches
- Android Evidentiary Locations
- Primary Evidentiary Locations
- Unique File Recovery
- Parsing SQLite Database Files
- Manual Decoding of Android Data
- Traces of User Activity on Android Devices
- Android Applications Store Data
- Deep Dive into Data Structures on Android Smartphones
- SMS/MMS , Calls, Contacts, and Calendar
- E-mail and Web Browsing
- Location Information
- Third-Party Applications
- Salvaging Deleted SQLite Records
- Salvaging Deleted Data from Raw Images on Android Devices
- Android Backup Files
- Overview of Backup File Forensics
- File Structures of Android Backups
- Locked Android Backups
- Data of Interest
- Google Cloud Data and Extractions
- Google Cloud Data Extraction and Analysis
- Bonus Materials
- Android Cheat Sheet
- Android Acquisition Methods
- Relevant White Papers and Guides
- Hands-on Lab to Pull Data from an Android Device

Module 7

Android File System Structures

- Data Structure Layout
- Physical
- File system
- Logical
- Data Storage Formats
- Physical and Logical Keyword Searches

Module 8

Handling Locked Android Devices

- Security Options on Android
- Methods for Bypassing Locked Android Devices
- Bypassing Android Security and Encryption

UCARA

Module 9

IOS (iPhone) Forensics

- IOS Encryption
- IOS File System Structures
- Define Data Structure Layout
- Data Storage Formats
- Parsing and Carving Data
- Physical and Logical Keyword Searches
- IOS Evidentiary Locations
- Primary Evidentiary Locations
- Unique File Recovery
- Parsing SQLite Database Files
- Manual Decoding of iOS Data
- Handling Locked iOS Devices
- Security Options on iOS
- Current Acquisition Issues
- Security Options on iOS
- Current Acquisition Issues
- Demonstration of Bypassing iOS Security
- Practical Tips for Accessing Locked iOS Devices
- Traces of User Activity on iOS Devices
- IOS Applications Store Data
- Apple Watch Forensics
- Deep Dive into Data Structures on iOS Devices
- SMS/MMS
- Calls, Contacts, and Calendar
- E-mail and Web Browsing
- Location Information
- Third-Party Applications
- Salvaging Deleted SQLite Records
- Salvaging Deleted Data from Raw Images
- Bonus Materials
- IOS Cheat Sheet
- Hands-on Lab to Pull Data from an IOS Device
- Manually Decoding and Interpreting Data from iOS Physical Data Dumps
- Manually Examining an Older File System Dump from an iOS Device
- IOS Acquisition Methods
- Relevant White Papers and Guid

Module 10

IOS File System Structures

- Data Structure Layout
- Physical
- File System
- Logical
- Data Storage Formats
- Physical and Logical Keyword Searches

Module 11

IOS Evidentiary Locations

- Primary Evidentiary Locations
- Unique File Recovery
- Parsing SQLite Database Files
- Manual Decoding of iOS Data

UCARA

Module 12

Retrieving User Activity Information IOS Devices

- IOS Applications
- Deep Dive into Data Structures on iOS Devices
- SMS / MMS
- Calls, Contacts, and Calendar
- E-mail and Web Browsing
- Location Information
- Third-Party Applications
- Retrieving Deleted SQLite Records
- Retrieving Deleted Data from Raw Images

UCARA

Module 13

IOS Backups, Malware and Spyware Forensics, and Detecting Evidence Destruction

- IOS Backup File Forensics
- Creating and Parsing Backup Files
- ICloud vs iTunes Data
- Verifying Backup File Data
- Locked iOS Backup Files
- Decrypting Locked iOS Backup Files
- Successfully Parse
- ICloud Data Extraction and Analysis
- Extract Cloud Data
- Parse Cloud Data
- Malware and Spyware Forensics
- Different Types of Common Malware
- Common Locations on Smartphones
- Analyze Using Reverse-Engineering Methodologies
- Detecting Evidence Destruction
- Different Types of Destruction Methods
- Determining When the Destruction Occurred
- Understanding What Happens When Data Are Destroyed
- Bonus Materials

Ducara Info Solutions (P) Ltd.

Any Query?

info@ducarainfo.com

www.ducarainfo.com

The Technology is changing every day and we at Ducara are committed to demonstrating values. Embracing a digital transformation strategy which drive returns on IT security investment.