Welcome to the **Oxygen Forensic® Device Extraction** training course!

This five-day instructor-led training event is geared toward students entering the mobile forensic arena that are ready to begin learning the art and science of acquiring data from phones or to simply broaden already existing knowledge. The course focuses on the physical, logical and OxyAgent methods of data extraction from Android and Apple iPhone devices using the **Oxygen Forensic® Extractor**, a component of the **Oxygen Forensic® Detective**.

Oxygen Forensic® Detective is the flagship technology of Oxygen Forensics and a world-class suite of tools that allow an investigator to ingest mobile device data from all industry standard extraction formats into a database architecture for single device analysis or multi-device analytics. The recent implementation of the x64 architecture of JetEngine elevates Oxygen Forensic® Detective to an unparalleled level of optimization, efficiency and analysis.

Students will perform hands-on problem solving and data extraction through industry standard methodology and equipment such as Emergency Download (EDL), ADB, Exploits, Boot loaders and other techniques. This course also covers the fundamentals of chain of custody, mobile device seizure best practices and evidentiary differences between acquisition methods.

The course also introduces **Oxygen Forensic® Detective** and prepares the student for the Oxygen Forensic BootCamp course.

Additional in-depth training available for Oxygen Forensic® Detective includes:

- Drone Analysis (one-day, instructor-led)
- Cloud Extraction (one-day, instructor-led)
- Passware Attacks (one-day, instructor-led)
- Call Detail Records (one-day, instructor-led)

Course Modules

Introduction to cell phone forensics

This module provides and overview of mobile device forensics, to include evidence handling, chain of custody, policies and procedures and methodologies for taking phones off the air to prevent changes after seizure. Students will get a firm grasp of the mobile device seizure process from crime scene to courtroom.

Cell phone technology

If you want to work for the fire department, you should understand fire. This module educates students about the technology that provides critical details about the best methods of extraction for any given device. Topics include:

- CDMA
- GSM
- iDEN
- MEID | MSN | FCCID
- Cell towers and network providers
- Other additional trace evidence items left over from connections

SIM, USIM, RUIM, CSIM

More acronyms. What are these? What evidence value do they provide? How are they dealt with relative to mobile device seizure and analysis? What is a PIN? What is a PUK? If this module description leaves you with any questions, you are in the correct class.

Install and Support

This module educates end-users about their customer experience with Oxygen Forensics while learning to install the latest Oxygen Forensic® Detective (OFD) products and mobile device drivers. Students will learn how to access their unique customer portal and download any software components needed.

Oxygen Forensic® Extractor – Technology Overview

This is the heart of the matter for this course. This module educates students on the use of **OFE** as the technology that allows them to acquire phone data. The options are vast and some of the methods are tricky, but that is the nature of this work. Students will finish this module understanding the capabilities of **OFE** and the workflow of importing **OFE** results into the **Oxygen Forensic® Detective**.

Evidentiary items of interest

In terms of "what we want", there are many pieces and parts in the process of evidence gathering. Goals of this module include understanding:

Logical memory	Calendars
Physical memory	Media files
Flash dumps	Applications
Hex dumps	Address books
Passwords / Security Pins	SMS and MMS messages
Deleted files | deleted data	Email messages
Data carving	File attachments
SIM cards	Global site tags

That list can look intimidating, but the goal is to provide many stones to overturn. The wider the net we cast, the more opportunity to find evidence we generate.

Data extraction from Apple devices

Rubber begins meeting the road in this module tooled around Apple iOS technology concerns and the need for iTunes as an acquisition technology. While not designed to make the student and Apple iOS professor, this module covers pertinent information about iOS environments to include

- iTunes backup data and locations
- Physical vs. logical extractions
- Accounts and passwords
- Login and tokens
- Decrypting iOS keychain data

As the culmination of acquisition, the resulting data is then ingested into **Oxygen Forensic® Detective** in preparation for analysis, analytics and reporting.

Data extraction from Android devices

This module is tooled around the Android OS and the methods by which Androids must be prepared for extraction. While not designed to make the student and Android OS professor, this module covers pertinent information about Android OS environments to include

- iTunes backup data and locations
- Physical vs. logical extractions
- Accounts and passwords
- Login credentials and tokens
- Decrypting content from the Android

Because of the large volume of different Android devices, OS versions, firmware packages, data protection schemes and potential proprietary features, many acquisition methods have surfaced to adapt to the ever-changing environment. Exploration of those methods will include:

- Introduction to JTAG (Joint Test Action Group)
- Introduction to ISP (In-System Programming)
- Introduction to EDL (Emergency Download Mode)
- Introduction to ADB (Android Debug Bridge)
- Introduction to Chip-Off
- Introduction to OxyAgent

As the culmination of acquisition, the resulting data is then ingested into **Oxygen Forensic® Detective** in preparation for analysis, analytics and reporting.

LG and other devices

This module expands into other phone types where chip-set recognition becomes essential, including identifying knockoffs and obscure or old OS devices. Students will build on previous module knowledge and apply alternate extraction methods (Logical / Physical / File System) to acquire data to be ingested in to **OFD**.

Analysis and reporting

This module highlights key areas of most commonly sought-after data of value.

- Calls
- Contacts
- Messages
- Appointment
- Media (Pictures | Videos)

Automated software is a must to normalize data from multiple formats or devices in preparation for analysis, but this module is designed to give students a good grasp of where those tools are looking during that normalization. Validation of process and recognition of source files are key components to the overall process.

The course concludes with a comprehensive oral and lab-based review.

Thank you for the interest in Oxygen Forensic® training.

Hope to see you in class soon!