OXYGEN
FORENSICS

Welcome to the **Oxygen Forensic® BootCamp** training course!

This three-day instructor-led training event is geared toward students that have a working familiarity with mobile device acquisition and extraction. This course does not provide hands-on extraction of mobile devices. That topic matter is available in the Oxygen Forensic® Data Extraction course. This course focuses on the analytic analysis and reporting capabilities of the **Oxygen Forensic® 12.0 Detective powered by JetEngine**.

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 import multiple extraction formats of Android, Apple and other data types while learning to use the suite of technology to develop workflows that will enable them to return to their environments and immediately apply new ideas.

In addition, students will leave this course with an Oxygen Forensics Learning Management System (LMS) account and in-depth preparation for the new **Oxygen Forensic® Detective** certification process based on the new version 12!

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 Record Analysis	(one-day, instructor-led)

Course Modules

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.

Technology Overview

It is not uncommon for end-users to not be fully aware of the analysis power at their fingertips when using Oxygen Forensic® Detective. This module provides exposure to all common technologies and tools included with the suite of technology that is the Oxygen Forensic® Detective. This exposure includes device acquisition and extraction analytic tools.

Configuration

Before using **OFD**, some initial conversation should be had regarding evidence storage, temporary workspace and machine capabilities. The **OFD** 12 technology includes many user-configurable options not previously available. This module provides instruction around those options, so end-users obtain maximum optimization for their environment needs.

Home Screen

The new **OFD** organizes all pertinent tools and interface functions in a new easy to use home screen. Students will learn to extract data, import existing industry standard data formats and utilize new and familiar workflows that can be applied as soon as they complete the course.

Import

The process of extracting | importing data is an integral part of the investigative process. In this module, students will extract data from previously acquired devices and begin familiarizing themselves with the new **OFD** interface and workflows that lead them directly to the most commonly sought-after investigation information.

Interface

Once those initial workflows are locked in, the rest of the interface becomes a command console of investigation and analysis. Students will learn the framework of columns, views and data sources that provide intuitive views in to extracted device data.

Sections

OFD automatically sorts through most commonly sought-after information organizing it into relevant sections. This organization includes normal feature-phone data such as calls, messages, media, contacts, etc. It also includes smart-phone relative data such as wireless connections, social interaction graphs, timeline capabilities and file explorer navigation. This module empowers the investigator with an array of tools and viewers to assist in information discovery and documentation.

Key Evidence

Speaking of documentation, **OFD** provides multiple methods of responsive data tracking. Users can “bookmark” files as “key evidence”. Files can also be simultaneously categorized by tag or label. Finally, investigators can add notes to any given item to help further qualify it for reporting or later review.

Data Export

This reporting wizard module demonstrates how to export data from a case into one of many output formats that can include graphics, hyperlinks and date | time filters. Reports can be modified to resemble corporate or agency logos and headers | footers while also being saved as templates for later use.

Search

OFD allows searching by keyword, keyword list, hash value and regular expression. In this module, students will create hash sets, observe pattern recognition via regular expression and discuss workflows that can decrease case turnaround time while allowing investigators the ability to do their own work faster than before without waiting on “lab results”.

Social Graph

The Social Graph analytic | interactive filter allows investigations to connect the dots like never before. Contact between individuals, groups and sources can be filtered for uniqueness or commonality. Filters can be tweaked by date and frequency of conversation while displaying the all-important lines of communication between contacts. This module deep dives in to merging contacts and filtering communications to establish patterns and links between contacts in one extraction or many.

Timeline

This analytic tool is a fan favorite and provides a chronological view of events of one data set or multiple. Everyone understands reading a book front to back. Displaying investigation details linearly is an easy method to follow. The Timeline also has tabs to filter relative data sets and can filter against one or multiple extractions. This module arms the investigator with another powerful tool for data presentation and culling.

Maps

No investigative technology is complete without the ability to plot points on a map. The **OFD** map technology blows past that standard by using those points to display common locations and routes using time and distance parameters. The map then blows that standard out of the water by providing the additional information of what actions were occurring to generate geo-relative data in those examples. Map data can be exported for 3rd party review and map projects can be saved for later retrieval. This module ensures the end-user of **OFD** will never be without these abilities again.

OFD Viewer

This workflow allows the technical side of the team to cull through masses of data to return more case-relative data to the investigator for review. The Viewer platform removes functions not relative to review, enabling the investigator to focus on the task at hand while using this client independent of the original OFD.

Use Your Powers For Good

This final module provides previews into alternate technologies that can assist with overt and possible covert investigations. End-users will learn how to configure OTG devices for credential recovery, in-the-field Android data collection, iTunes backup discovery and other application artifact collection. Password protected backups will be addressed, and workflows for drone data recovery, cloud extraction and call detail records (cell tower data) will be introduced. This module also introduces students to the powerful facial recognition technology included in the tool suite.

The course concludes with a comprehensive oral and lab-based review that will also help prepare students for the version 12 certification process.

Students leave this event with an account in the Oxygen Forensics Learning Management System, an 'On The Go' (OTG) USB device and several resources for mobile forensic email lists and websites, including how to submit feature requests and support tickets with the Oxygen Forensics Support team.

Thank you for the interest in Oxygen Forensic® Detective training.

Hope to see you in class soon!