OXYGEN FORENSICS

Welcome to the Oxygen Forensic® Detective - **Accelerated Training Program**!

The OFD-ATP is a five-day instructor-led training event that includes extensive education on Oxygen Forensic® Extractor and its abilities to extract logical, physical and agent-based data dumps from iOS, Android and KaiOS devices. Those two days are the essential precursor to the next three days of honing analytic analysis and reporting capabilities of the Oxygen Forensic® Detective.

Oxygen Forensic® Detective is the flagship technology of Oxygen Forensics and a world-class suite of analytic 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 extract and import multiple formats of Android, iOS and other data types and learn 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 workflows and tools included with the suite of technology that is the Oxygen Forensic® Detective, including device extraction and analytics.

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.

Device Extraction

The top rung of the mobile forensic ladder is device extraction. Art, science, research, luck, star alignment and technology combine to present investigators and examiners with some of the most challenging of tasks when it comes to extracting data from handsets, tablets, drones and peripherals. In this module, students will learn about the major challenges faced with extraction, as well as "where to start" down the path of success when extraction is required. While not all inclusive (there is a five-day training course for that), this module arms the student with the ability to get productive as soon as they finish the course. Topics covered include iOS, Android and KaiOS device access and the differences in extraction type, including physical, filesystem and logical. This module includes hands-on Checkra1n device exploit and extraction as well as root extraction of Android and KaiOS devices.

Extraction Import

The process of extracting | importing data is an integral part of the investigative workflow. In this module, students will import data from previously acquired devices and begin familiarizing themselves with the **OFD** interface and workflows that lead them directly to the most commonly sought-after investigation information. The OFD import capability also allows the user to import several industry-standard technology datasets, including the new disk archive file format – 'dar', as well as many peripheral file types and even loose files for analysis.

Users can also import search warrant returns, allowing the analytics and easy categorization and correlation on data the many times is large, cumbersome, unorganized and difficult to report on. Instagram and Facebook lead this charge but watch the list to grow!

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.

Overview Information

OFD provides the investigator with an immediate "heads-up" view of evidence information, owner information and accounts, extraction information, top-10 categories (apps, groups, users). All this information can be included in reporting, but prior to reports, this section can provide a well-rounded look at the device and its user(s).

General Sections

OFD automatically sorts through most commonly sought-after information and organizes 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 data, applications and more. This module empowers the investigator with an array of tools and viewers to assist in information discovery and documentation. General Sections include:

- Calls
- Reports
- Contacts
- Messages
- OS Artifacts
- WebKit Data
- Flight Logs
- Applications
- Apple Notes
- Wireless Connections
- Accounts | Passwords
- Media (pictures | video | audio)

Analytics

Today's investigation data can be complex, large and overall daunting when it comes to analysis and documentation of multiple devices, users and applications. OFD leads the industry in data analytics and this module educates users on the abilities at their fingertips. Mastery of OFD analytics will take your final work product places it's never been in terms of link analysis, geographic coordination, chronologic discovery and biometric and categoric recognition. Students will add the following technologies to their investigative arsenal:

- Timeline
- Social Graph
- Facial Categorization
- Image Categorization
- Multi-faceted Search
- Key Evidence Manager

Tools

In concert with the analytic tool chest, OFD provides an additional layer of expert technologies to assist with data normalization, deep-dive data recovery, alternate platform data extraction, in-the-field data extraction, credential and token acquisition and so much more. Students will learn the following toolbox additions:

- Oxygen Forensic® Maps
- Oxygen Forensic® KeyScout
- Oxygen Forensic® OxyAgent
- Oxygen Forensic® Plist Viewer
- Oxygen Forensic® SQLite Viewer
- Oxygen Forensic® Cloud Extractor
- Oxygen Forensic® Call Data Expert

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. The OFD report wizard specializes in reducing the unwanted noise data around items of importance. Specificity becomes key when data is organized with the report wizard's abilities.

OFD Viewer

The OFD Viewer 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.

Additional Technology

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 and will be introduced. ***Use your powers for good*** in this module!

Appendix A – Comprehensive Lab

In this lab, students will simulate challenging the Oxygen Forensic Certification with data not previously used in class. This simulation is covered as a group but designed to prepare the student for certification after course conclusion.

Appendix B – Comprehensive Review

This oral review reinforces the objectives of each module in an instructor-led conversation that keeps key points of understanding at the learning forefront.

Appendix C – Mobile Forensic Resources

This final module provides information on where to get started when a phone pops into evidence to include mobile forensic sites and Oxygen Forensic® specific help and support sites. Ad as always, you are always welcome at Oxygen Training …

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

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