Welcome to the **Oxygen Forensic® Boot Camp** training course!

This three-day instructor-led training event is geared toward students that have a working familiarity with mobile device extraction and analysis and focuses on extraction, use-case, and reporting capabilities 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 industry standard extraction formats into a database architecture for single device analysis or multi-device analytics.

Students will begin by learning to extract an iOS and Android device and import multiple extraction formats of Android, Apple and other device and data types. The course continues with students learning core technology allowing them organize data, streamline workflows and learn reporting methods 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 Oxygen Forensic® Detective certification process!

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

• OFDA – Oxygen Forensic® Drone Analysis	(1-day, instructor-led)
• OFCE – Oxygen Forensic® Cloud Extraction	(1-day, instructor-led)
• OFAA – Oxygen Forensic® Advanced Analysis	(3-day, instructor-led)
• OFXiB – Oxygen Forensic® Extractor in a Box	(3-day, instructor-led)

All courses can be accessed buffet-style at a fixed price with a Training pass.

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.

Configuration

Before using **OFD**, some initial conversation should be had regarding evidence storage, temporary workspace and machine capabilities. **OFD** technology includes many user configurable variables. This module provides instruction around those options, so end-users obtain maximum optimization for their environment needs.

Device Extraction

This module educates students about how to get started with the **Oxygen Forensic® Extractor**. Students will learn how to create an iTunes backup of an Apple device as well as how to prepare an Android device for multiple extraction methods. Specific additional topics covered in this module include:

- iTunes backup data and locations
- Encrypted vs non-encrypted backups
- Android Developer settings and USB debugging
- The risks of reset – even as the last resort

large focus of this module educates students on the use of Oxygen Forensic® Extractor as the technology that allows them to extract device 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 many capabilities of the OFE and the workflow of importing OFE results into the Oxygen Forensic® Detective

Import

In this module, students will import data from previously extracted devices and begin familiarizing themselves with the **OFD** interface and workflows that lead them directly to the most commonly sought-after investigation information. Import "type" information includes:

- Apple systems including GrayKey
- Android systems including bin files and backups obtained by other means
- Drone data including DJI and Parrot
- KaiOS data – physical and filesystem data
- Desktop extractions from KeyScout and .e01 files
- Memory cards | SIM cards and folder contents
- Warrant returns including Facebook, Instagram, Snapchat, and Twitter
- Third party extractions including UFED data, XRY backups and Meiya Pico

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 and top-10 categories (apps, groups, users). This information can be included in reporting and provides 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
- Contacts
- Messages
- OS Artifacts
- WebKit Data
- Reports
- Calendar
- Snapshots
- Flight Logs
- Call Data Records
- Applications
- Apple Notes
- Wireless Connections
- Accounts | Passwords
- Files (categorized by tab)

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 has never been in terms of link analysis, geographic coordination, chronologic discovery and biometric, categoric and optical character recognition. Students will add the following technologies to their investigative arsenal:

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

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 gain familiarity with mapping geo-location data, viewing database file structure and gathering account credentials.

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**.

Appendix A – Comprehensive Lab
Appendix B – Creating a Checkra1n USB
Appendix C – Resources

Students leave this event with an account in the Oxygen Forensics Learning Management System 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.