Welcome to the **Oxygen Forensic® Advanced Analysis** (OFAA) training course!

This three-day instructor-led training event is a direct successor to the three-day OFBC course and continues with deep dives into Oxygen Forensic® Detective analytics, database parsing, lost data recovery, alternate data sets and advanced tools such as the Call Data Expert, the SQLite and Property list viewers and Oxygen Maps. Students will investigate IoT devices, application cache database files with the SQLite database and Property list viewers and learn to aggregate and correlate data from multiple sources to enhance the overall investigation in scenario-based exercises.

A solid understanding of Oxygen Forensic® Detective will greatly enhance the deliverables of this course! 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.

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

- OFBC – Oxygen Forensic® Boot Camp (3-day, instructor-led)
- OFDA – Oxygen Forensic® Drone Analysis (1-day, instructor-led)
- OFCE – Oxygen Forensic® Cloud Extraction (1-day, instructor-led)
- OFXiB – Oxygen Forensic® Extraction in a Box (3-day, instructor-led)
- OFDV – Oxygen Forensic® Detective Viewer (1-day, instructor-led)

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

This course prepares the student for the OFC recertification process!

Course Modules

Install and Support

This module educates end-users about how to install the latest Oxygen Forensic® Detective (OFD) products and mobile device drivers. Students will learn how to access their unique customer portal to download software and drivers. Additional software will also be described and installed for additional extraction flexibility.

Technology Review

- Passware Mobile Kit
- Oxygen Forensic® Map
- Oxygen Forensic® KeyScout
- Team Win Recovery Project
- Oxygen Forensic® SQLite Viewer
- Oxygen Forensic® Cloud Extractor
- Oxygen Forensic® Call Data Expert
- Oxygen Forensic® Property List Viewer

Use Case | Investigation #1

Jumping right into things, the first scenario to work through includes data from IoT devices including Amazon, Google, and Ring. This scenario involves collaboration with a computer forensic unit and includes expanded education and lab work with:

- Oxygen Forensic® KeyScout
- Oxygen Forensic® Cloud Extractor
- Computer hard disk drive evidence files

Use Case | Investigation #2

The next case includes intensive SQLite database interrogation. As the investigator, you will be assigned on the job education on SQLite database structure, content and viewing methodology. That knowledge will be applied to assist in locating target data from "non-parsed" target files. This scenario involves expanded education and lab work with:

- Oxygen Forensic® SQLite Viewer
- Oxygen Forensic® Property List Viewer

Use Case | Investigation #3

This scenario challenges the analyst to discover as many things in common as possible between seemingly uncommon targets in a limited time.

Use Case | Investigation #4

This team challenge includes OxyAgent extraction, multiple devices and collaborative problem solving to get the most data possible from devices not willing to participate in the challenge! This challenge includes expanded education with:

- Oxygen Forensic® OxyAgent

Use Case | Investigation #5

Back to database interrogation. We will continue applying what we've learned with additional database parsing

- Oxygen Forensic® SQLite Viewer
- Oxygen Forensic® Property List Viewer

Use Case | Investigation #6

With a computer, a large challenge could be – "Who was at the keyboard at the time of the crime?". With a phone, a large challenge could be – "Who was using the phone at the time of the crime?". Pretending you have figured that out, now you must answer – "Who's not telling the full story, the user, the device or the call detail records? This challenge includes expanded education and timeline re-creation with:

- Mobile provider records
- Oxygen Forensic® Call Data Expert

Use Case | Investigation #7

So – whatever you just found is locked -- Augh! – Now what? This challenge includes expanded education with:

- Passware Mobile Kit
- Oxygen Forensic® KeyScout

Use Case | Investigation #8

Using the Team Win Recovery Project (TWRP) to your advantage. What is TWRP you say? It is an opensource, free, custom recovery image for android. TWRP provides options when most other options have not been successful.

- Gaining device access with TWRP
- Extracting device data with TWRP

Use Case | Investigation #9

This scenario involves an investigation where all chatting and media exchange took place in WhatsApp. The device hosting WhatsApp no longer has the application installed but a token was captured from a device backup and stored in a Google account. Follow the process from discovery of the token to extracting, decrypting, and parsing the database. This challenge explores the WhatsApp capabilities of the Oxygen Forensic® Cloud Extractor.

Use Case | Investigation #10

Bonus challenge! This lab explores some of the more common device applications today. These application artifacts will be explored via the Applications section of OFD and reported via the Export wizard.

- Viber
- Telegram
- Facebook
- WhatsApp

This course concludes with a "**Capture the Flag**" challenge that exposes students to scenario data that may help prepare them for OFC recertification.