

## XiB Course Description

Welcome to the **Oxygen Forensic® Extraction in a Box (XiB)** training course!

This three-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 extracting data from phones or to broaden existing knowledge of **Oxygen Forensic® Extractor**. The course focuses on the physical, logical and OxyAgent methods of data extraction from Android, Apple and KaiOS devices, as well as peripherals such as drones, SD cards and SIM cards 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 industry standard extraction formats into a database architecture for single device analysis or multi-device analytics.

Students will perform hands-on research and data extraction through industry standard methodology, exploits, and other avenues such as Emergency Download (EDL), ADB, and Common Vulnerabilities and bypass techniques. This course also covers the fundamentals of FDE (full disk encryption), FBE (file-based encryption) and the methods of successful decryption techniques using Oxygen technology in the lab (meaning you may no longer be sending those phones away for paid help).

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)
- OFXiB – Oxygen Forensic® Extraction in a Box (3-day, instructor-led)
- OFAA – Oxygen Forensic® Advanced Analysis (3-day, instructor-led)
- OFBC – Oxygen Forensic® Boot Camp (3-day, instructor-led)
- OFDV – Oxygen Forensic® Detective Viewer (1-day, on-demand)
- OFAT – Oxygen Forensic® Agent Triage (1-day, instructor-led)
- OFDP – Oxygen Forensic® Data Presentation (1-day, instructor-led)
- OFKC – Oxygen Forensic® KeyScout Collection (1-day, instructor-led)
- OFAI – Oxygen Forensic® Analytic Investigation (1-day, instructor-led)

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

When this class is delivered remotely, a package including the required cables, devices and peripherals is sent to the student for hands on extraction with their live instructor. This box returns to Oxygen Forensics at course end.

## Course Modules

### Install and Support

This module provides an overview of **Oxygen Forensic® Extractor** and mobile device forensics and extraction. Students will learn about the objectives of the course from A-Z including installing unsigned device drivers, using ADB commands, configuring Extractor for best success and maintaining data integrity.


### Where to Begin

When a device lands at your feet, the next step is research. The information you determine about the device helps drive your interaction with its data extraction process. The research may involve websites, phone labels, internal information and identification marks or ports. This module helps in finding:

- Make
- Model
- Chipset
- Operating system
- Exploit applicability
- Extraction methodology

### Oxygen Forensic® Extractor

This module provides an overview of the Oxygen Forensic® Extractor interface – students become familiar with the following interface options:

- Exploits
  - Restorations
  - Device Support
  - Extraction hashing
- 

## Where to begin?

This module is at the heart of device extraction and brings to light many of the challenges, including:

- Terminology
- Device Types
- Extraction Types
- Driver challenges
- Cable challenges
- Exploit challenges

The extraction methods employed are dictated by the device and data available. This discussion will include those relative topics for Apple, Android, KaiOS, drones and peripheral devices – also documented in this table:

|                | “Physical”        | “Logical” | Agent | Other                   |
|----------------|-------------------|-----------|-------|-------------------------|
| <b>Apple</b>   |                   | X         |       | <b>Checkra1n</b>        |
| <b>Android</b> | X                 | X         | X     |                         |
| <b>KaiOS</b>   | X                 |           |       |                         |
| <b>Other</b>   | <b>SD   Drone</b> |           |       | <b>MTP   UICC   APK</b> |

This module also presents itself under the analogy that if you want to work for the fire department, you should understand fire. Students will learn about how to research device characteristics that will expose critical details about the best extractions for that device – to include:

- IMEI data
- Encryption type
- Firmware flashing
- BFU vs. DFU
- Download agents
- Common Vulnerabilities and Exposures

## Passware Kit Mobile

This module focuses on the OEM Passware technology included in **Oxygen Forensic® Detective**. Content includes:

- Understanding the interface
- Creating custom dictionaries
- Creating custom attack profiles
- Configuring for performance

This module also discusses password protected backups, brute force vs. dictionary attacks and how and when to use Passware during the device extraction process to attack full disk and file-based encryption keys to defeat secure-boot environments.

## Android Preparation

This module focuses on the research of Android devices to ensure one is armed with the best information to determine the best approach to the device in hand. Content includes:

- Determining phone information
- Enabling 'Developer mode'
- Entering USB debugging mode
- Troubleshooting authorization
- Understanding Android extractions by brand | model | SoC | exploit

This module also discusses the resources, websites, and ways to determine the proper qualifying data about a device that will drive toward the best extractions.

## Android Debug Bridge

This module focuses on ADB commands and using the Android Debug Bridge software installed with **OFD**. Commands and features include:

- Adb devices
- Adb kill-server
- Adb -s shell getprop
- Adb reboot edl | Adb reboot download | Adb reboot-bootloader
- Adb shell getprop ro.crypto.state
- Adb shell getprop ro.crypto.type

**The remainder of class time is used to perform hands on extractions using the supplied XiB box contents. The extraction order and timing are at the instructor's discretion based on course breaks, password attacks, troubleshooting, etc.**

## Data extraction from Apple devices

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

- iTunes backup data and locations
- Encrypted vs non-encrypted backups
- Logical file structure extraction
- Full file system extractions
- iOS keychain data extraction
- The risks of reset – even as the last resort

Students will perform hands-on iTunes backups, logical file structure extractions, Checkra1n exploits and Secure Enclave Processor (SEP) exploits (lock code recovery).

## Data extraction from Android devices

This module is toolled around the Android OS and devices and covers the methods by which Androids can be prepared for extraction, exploited by common vulnerability exposures, and directly attacked with Passware to recover screen lock pins / passwords or swipe codes to attack file-based and full disk encryption environments. While not designed to make the student an Android OS professor, this module covers pertinent information about Android OS extractions, to include:

- **Android physical (via ADB)**
- **Android backup (via ADB)**
- **Android OxyAgent extraction**
- **Android manual OxyAgent extraction**
- **Android OxyAgent over Wi-Fi extraction**
- **Android file system**
- **Samsung Android**
- **Samsung Exynos**
- **Huawei Kirin**
- **Sony MTK**
- **APK Downgrade**

Students will perform hands-on backups, logical file structure extractions, and physical device extractions, as well as device, SoC and brand specific exploits, including application downgrades and OxyAgent extractions using **Oxygen Forensic® Extractor**.

## Other Extractions

This module covers the “Other” category in **Oxygen Forensic® Extractor**.

- **KaiOS**
- **MTP**
- **Memory Card**
- **UICC**

Students will perform a physical extraction of a KaiOS device, a logical extraction of media file types via MTP, a physical extraction of an SD memory card (including data recovery for deleted files) and an adapter specific extraction of a UICC (SIM card).

Students leave this course with LMS access to the remaining **Oxygen Forensic® Extractor** extractions not performed as hands-on labs during this course.

**Thank you for the interest in Oxygen Forensic® Training.**

---

***This course runs in the classroom and remotely***

In times like these, when it is difficult to make it to the classroom, we are sending the classroom to you! Using our innovative XiB concept, we can learn to extract together, with students and instructor using the same hardware to learn! The kit includes phones, cables, tweezers, SIM and SD-card readers, an OTG device, a PPE pack and much more! **XiB – Extraction in a Box ... experience it!** (return shipping label included)

