Welcome to the **Oxygen Forensic® Device Extraction** (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 will no longer be sending those phones away for paid help).

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)
- OFAA – Oxygen Forensic® Advanced Analysis (3-day, instructor-led)

This course is currently being offered remotely by sending a box of cables and devices to the student for hands on extraction with their live instructor. This box returns to Oxygen Forensics at course end.

Course Modules

Introduction to cell phone extraction

This module provides an overview of mobile device forensics and extraction, to include the primary adversaries of extraction and the tactical methods that can pierce their defenses – topics include:

- OS Type
- OS Version
- Security Patches
- Firmware
- Encryption
- Lock codes
- Drivers
- Cable types
- Protocols and modes

If you want to work for the fire department, you should understand fire. This module also educates students 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

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.

Oxygen Forensic® Extractor – Technology Overview

This is the heart of the matter for this course. This module educates students on the use of **OFE** 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 the capabilities of **OFE** and the workflow of importing **OFE** results into the **Oxygen Forensic® Detective**.

Extraction types

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. Topics include:

	"Physical"	"Logical"	Agent	Other
Apple		X		GrayKey | Checkm8
Android	X	X	X	
KaiOS	X			
Other	SD | Drone			UICC | Sim

This table can look intimidating, but the goal is to provide many stones to overturn. The wider the net we cast, the more opportunity to extract data we generate.

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
- Extracting full file systems
- Extracting iOS keychain data
- The risks of reset – even as the last resort

Students will perform hands-on iTunes backups, logical connections and Checkra1n exploits using **Oxygen Forensic® Extractor**.

Data extraction from Android devices

This module is tooled around the Android OS and the methods by which Androids can be prepared for extraction. While not designed to make the student an Android OS professor, this module covers pertinent information about Android OS environments to include:

- Developer settings and USB debugging
- ADB – Android Debug Bridge
- Physical vs. logical extraction considerations
- Phone brands vs. systems on chip methods
- Decrypting content from the Android
- Shorting test points to enter download mode

Because of the large volume of different Android devices, OS versions, firmware packages, data protection schemes, proprietary features and chip sets, many extraction methods have surfaced to adapt to the ever-changing environment. Exploration of those methods will include:

- Brand exploits (LG, Motorola, Sony, Huawei, Samsung)
- Chipset exploits (Exynos, Kirin, MediaTek, Spreadtrum, Qualcomm)
- Android debugging (Common Vulnerabilities and Exposures | backups)
- OxyAgent extraction (Tethered | In the field | Wireless)

Students will perform hands-on extractions of Samsung, Huawei, Nokia, Sony and Alcatel devices using **Oxygen Forensic® Extractor** and the **OxyAgent**. Methods will include configuring and using an OTG (on the go) device, navigating internal device hardware to short phone test points to enable device download mode, and extracting data over a wireless network.

Other devices

This module expands into other devices. Learning objectives include:

- **Drones** (controllers | UAVs)
  Understanding the difference between logical drone data and physical drone data when comparing cloud extracted data and drone extracted data. Understanding the process of exploiting and extracting the drone OS.

- **SD Cards** (from phones and drones)
  Understanding the physical extraction aspect of SD cards.

- **SIM Cards** (UICC cards from handsets)
  How does one read the content of a SIM card? What evidence value do they provide? What is a PIN? What is a PUK?

- **KaiOS devices** (not quite iOS | not quite Android)
  Learning to research and physically extract a KaiOS device

Applied decryption

This module discusses how to best configure your decryption | key-recovery efforts when it comes to attacking secure boot environments or file-based encryption schemes with the **Passware Mobile Kit** (included with Oxygen Forensic® Detective).

Topics include:

- Social engineering
- Full Disk Encryption
- File-Based Encryption
- Dictionary creation
- Distributed processing
- Bypassing: Pins | Passwords | Swipe Codes

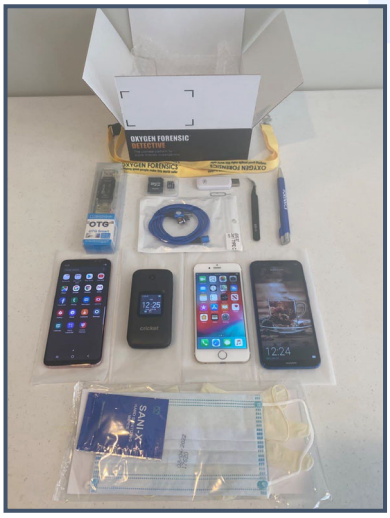
Data integrity and Concurrent activity

This module provides understanding of best practices of maintaining extraction integrity and managing databases and case organization. Additionally, the tips and tricks to concurrent extraction are covered so students can begin multi-tasking as soon as they are back in the lab.

The course concludes with a comprehensive oral and lab-based review.

Thank you for the interest in Oxygen Forensic® Training.

Special note for 2021



In times like these, when it is difficult to make it to the classroom, we are sending the classroom to you! Using our innovative remote training labs, combined with sending you the lab equipment, 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 and a PPE pack.

XiB – **Extraction in a Box** … experience it!
(return shipping label also included)