CORELLIUM®

Mobile Security Education & Training

Corellium gives educational institutions, professors, and trainers a powerful platform to teach computer science and software development without physical devices. Spin up any combination of device and OS and use Corellium's built-in research and teaching tools, all through simple browsers.

The Corellium Arm virtualization platform provides never-before-possible mobile device training environments through the use of virtual iOS and Android phones. Its high-accuracy, Arm-native phone virtualization allows instructors to effortlessly provide real-world, hands-on mobile security and app development training without the typical challenges or limitations of using software emulators.

It's not an emulator; it's Arm on Arm virtualization.

Limitless Teaching On Virtual Phones

Corellium provides a powerful and polished user interface with built-in teaching tools for root access, app forensics, file system manipulation, Frida instrumentation, network traffic analysis, and much more. Corellium's comprehensive API and USBFlux technology streamlines integration with leading development, security, and educational tools — such as Xcode, Android Studio, IDA Pro, Burp Suite, Charles Proxy, and more.

Offer New Courseware

Corellium virtual devices are a drop-in replacement for physical devices, integrating seamlessly with existing curricula. And if you don't currently offer mobile security and research courses, imagine the possibilities.

Corellium offers mobile security training classes of its own to help you on your way. Feel free to take our classes, and then contact us for potential use of our syllabi and materials to create or jumpstart your own courseware.

Industries

- Online Academies & Courseware
- Colleges and Universities
- Mobile Security & Developer Teams

Roles

- Computer Science Professors
- Mobile Security Training Professionals
- Cybersecurity Consultants
- Security/IT Instructors

Why Choose Corellium for Education & Training?

On-Demand Access

Skip the setup process and start teaching immediately with pre-built device snapshots.

Lower Costs

Remove the overhead of physical devices with a platform that requires only a web browser for both teachers and students.

Simplify Teaching and Learning

Easily train every student on the same device image and configuration, regardless of class size.

Train on Any Version

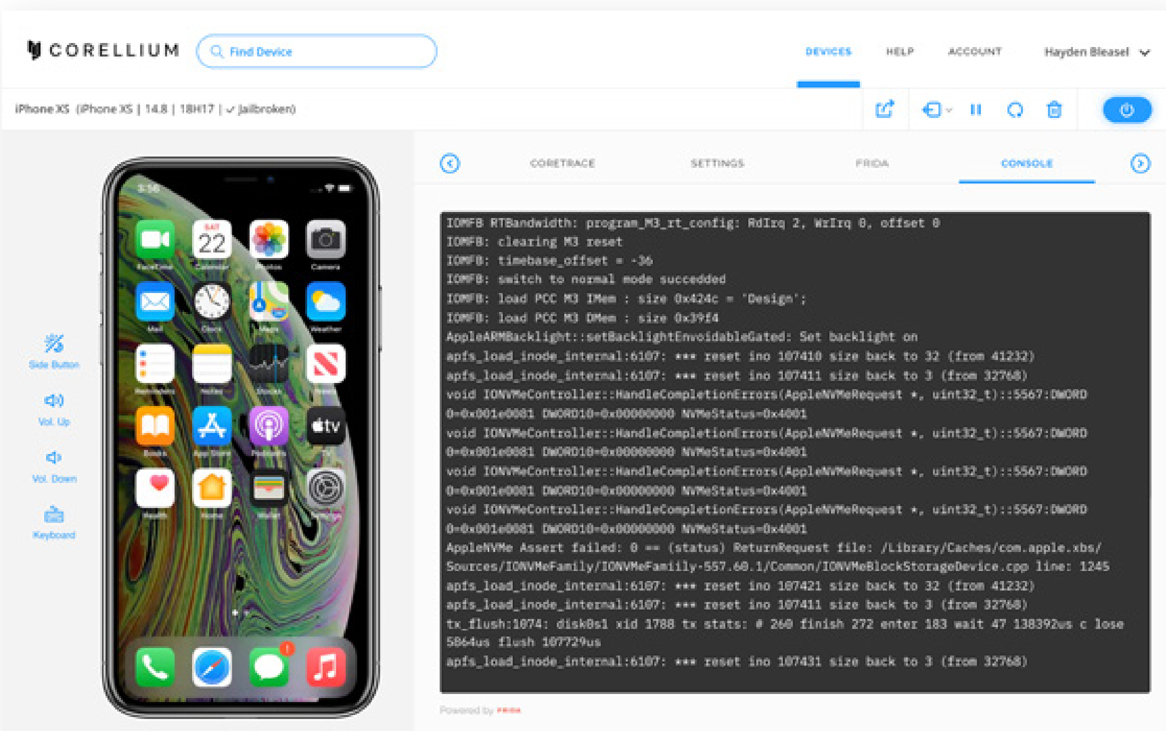
Provide security training on both iOS and Android with a near-limitless combination of device models and OS versions.

No Physical Phones

Give each student a virtual device to work with so you no longer need to worry about physical devices.

Root Access & Jailbreak

Teach at the kernel, file, system, app, and network layers with the only solution that provides both instant root and jailbreak access.



Courseware Topic Examples

- Mobile App Penetration Testing
- Dynamic App Security Testing (DAST)
- Mobile Data Privacy & Compliance Testing
- OWASP MASVS and MSTG Best Practices
- Ethical Hacking for Mobile
- Mobile Malware Detonation and Analysis
- Mobile OS, Memory, and I/O Structures
- SSH and VPN Device Connectivity
- iOS and Android App Signing
- Network Traffic Interception and Tracing
- SSL Certificate Pinning & Validation
- Capture-the-Flag (CTF) Exercises

Developer Tool Examples

- Xcode and the LLDB debugger
- Android Studio and the Java debugger
- Appium for app test automation
- MobSF for DAST and SAST
- Burp Suite for app pentesting
- Charles Proxy for network traffic analysis
- Frida for dynamic instrumentation and scripting
- IDA Pro for debugging and reverse engineering
- Binary Ninja for vulnerability research
- Cydia as an Advanced Packaging Tool (APT)

Free trials at **Corellium.com**

CORELLIUM ®