CORELLIUM®

Mobile App Penetration Testing

The Corellium Arm virtualization platform provides never-before-possible mobile app penetration testing on virtual iOS and Android devices. Its high accuracy, Arm-native model enables static and dynamic app vulnerability discovery and exploitation testing.

**It’s not an emulator or a simulator;
it’s Arm on Arm virtualization.**

iOS and Android Virtual Devices On-Demand

The Corellium hypervisor for Arm (CHARM) runs on native Arm processors, available in the cloud or as onsite server appliances. Corellium provides a single platform for iOS and Android virtual devices that are a drop-in replacement for physical devices. Simply spin-up a near limitless combination of device and OS, from older versions to the very latest, patched or unpatched, jailbroken or not.

Comprehensive Penetration Testing

Corellium provides a powerful and polished user interface with built-in security tools for root access, forensic analysis, filesystem manipulation, Frida scripting, SSL/TLS stripped network monitoring, application debugging, and much more. A comprehensive API and USBFlux technology enables integration with leading development and security tools such as Xcode, Android Studio, IDA Pro, Frida, and Burp Suite.

Industries

- ✓ Enterprise
- ✓ Security Service Providers
- ✓ Independent Consultants
- ✓ Government

Roles

- ✓ Mobile App Pentesters
- ✓ Mobile App Forensics
- ✓ Vulnerability Researchers
- ✓ Red & Blue Teams

Why Choose Corellium for Mobile App Pen Testing

Virtualization Not Emulation

ARM-native, this is real pentesting on virtual devices with the ability to quickly load your own binaries.

Spin-Up Needed Devices

Easily spin-up near limitless combinations of devices and operating systems, from past models and releases to the very latest.

Instant Root & Jailbreak Access

Root any device configuration, including the latest versions of iOS, even when no public jailbreak is available.

Dynamic Pen Testing

Built-in network monitoring tools lets you analyze encrypted application traffic instantly.

Static Pen Testing

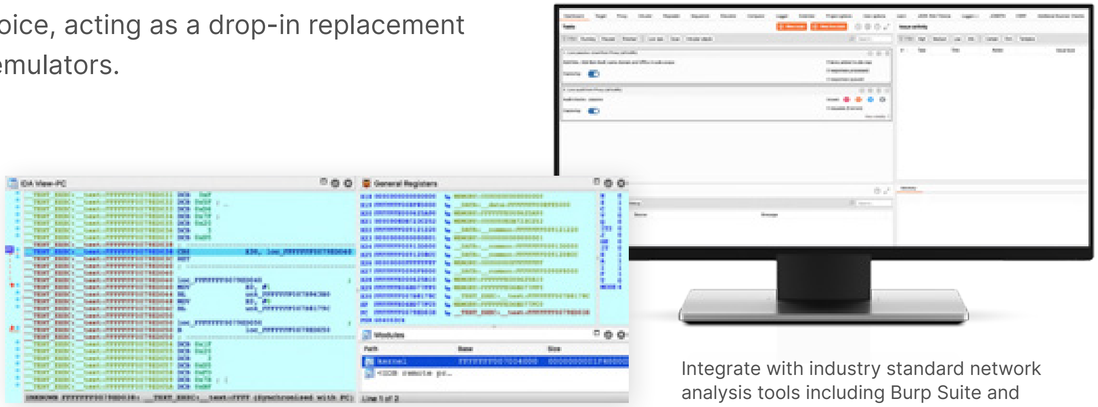
Direct root file system access for Android and iOS devices to perform application static analysis and mobile forensics.

API and Integrations

Powerful API for scripting and integrations with testing tools such as Frida, Burp, IDA Pro, GDB/LLDB, Xcode, and Android Studio.

Use with your favorite tools

Corellium's virtual devices are designed to integrate seamlessly with existing tools of choice, acting as a drop-in replacement for physical devices or emulators.



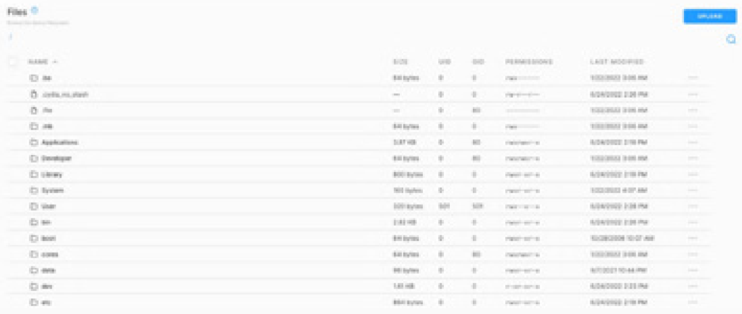
Integrate with your favorite tools for binary disassembly including IDA Pro.

Integrate with industry standard network analysis tools including Burp Suite and Charles Proxy.

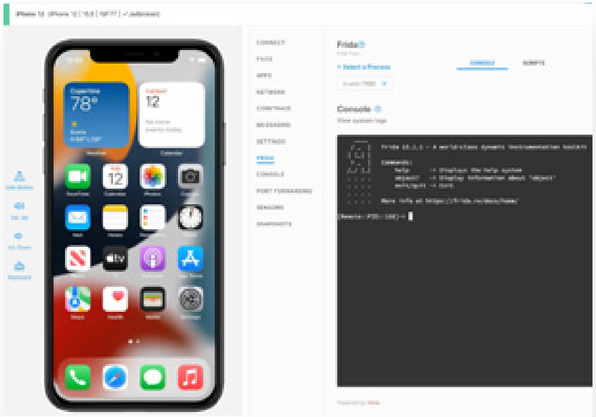
Technical Capabilities

Mobile App Penetration Testing

- ✓ Easily spin-up near limitless combinations of iOS and Android device, OS and mobile apps
- ✓ Gain device root access, no need to apply additional code or tools
- ✓ Test mobile apps on any OS version; jailbroken, rooted or not
- ✓ Test enterprise mobile apps (IPAs and APKs)
- ✓ Network traffic interception and SSL/TLS stripping
- ✓ Integration with Burp Suite, Charles Proxy, and Frida
- ✓ Browse the device's file system - download and forensically examine files
- ✓ Research and test new and known exploits
- ✓ Control device sensors, GPS location, and device IDs
- ✓ Script and API capabilities to automate testing



Integrate with industry standard network analysis tools including Burp Suite and Charles Proxy



```
Frida 15.1.1 - A world-class dynamic instrumentation toolkit

Commands:
    help      -> Displays the help system
    object?   -> Display information about 'object'
    exit/quit -> Exit

More info at https://frida.re/docs/home/
[Remote::PID::[illegible]]->
```

Root level device access with the ability to upload and download local files.

Training & Education

- ✓ Mobile app penetration training
- ✓ Inject artificial vulnerabilities for training
- ✓ Perform capture-the-flag (CTF) exercises
- ✓ Teach mobile app security and development best practices

Compliance & Auditing

- ✓ Regulatory pentesting, standards development, and auditing
- ✓ Data privacy testing and auditing

SPONSOR OWASP

Corellium Virtual Hardware Platform

VIRTUAL DEVICES
Arm-powered phones and IoT devices with endless OS and model combinations.

HYPERVISOR
Corellium Hypervisor for Arm (**CHARM**) is a type 1 hypervisor and the only one of its kind.

ARM SERVER
Virtual models run on Arm, just like real devices, combining native fidelity with on-demand availability.

- TOOLING
  Simplified connection of IDE, debugging, network and security tools and comprehensive APIs.
- CONTROL
  Configure device buttons, sensors, location, environment, battery, device IDs, ports, cameras and mics.
- X-RAY VISION
  Powerful OS, app, file, system call, and console access and control.
- INTROSPECTION
  Advanced OS, kernel and boot control and tooling.
- NETWORK ANALYSIS
  HTTP/S traffic inspection, tracing, and logging.
- REPLICATION
  Snapshot, clone, and restore device states.
- TEAMING
  Easy project workspace management and team collaboration.
- ROOT ACCESS
  Root or jailbreak devices instantly, no need to add code or apply security vulnerabilities.

AMPERE

Corellium Appliances

Corellium appliances for onsite and air-gapped solutions run on the latest Ampere Altra Arm servers.

aws

Corellium Cloud

Corellium is hosted on AWS using Amazon Graviton Arm servers. Customer private AWS Graviton clouds also supported.

CORELLIUM ®