

Mobile Vulnerability Research

The Corellium Arm virtualization platform provides never-before-possible security vulnerability research for iOS and Android phones with deep forensics and introspection tools.

Its high accuracy, Arm-native model enables real platform vulnerability discovery and exploit validation.

**This is not an emulator or simulator —
it's Arm on Arm.**



This is basically magic.

- MARK DOWD, AZIMUTH SECURITY

Virtual iOS and Android Devices On-Demand

The Corellium hypervisor for Arm (CHARM) runs on native Arm processors, in the cloud or on server appliances. A single platform supports high-fidelity security tooling for both iOS and Android phones and tablets. Simply spin-up a near limitless combination of device and OS, from older versions to the very latest, patched or unpatched, jailbroken or not.

Cutting-Edge Vulnerability and Exploit Research

Corellium provides a powerful and polished user interface with built-in security tools for root access, process tracing, file system manipulation, Frida scripting, TLS-stripping network monitoring, kernel debugging, SEP/iBoot debugging, and much more. Combined with a comprehensive API and USBFlux technology, integrating with leading development, security, and forensics tools such as Xcode, Android Studio, IDA Pro, and GDB/LLDB is seamless.

Industries

- ✔ Government
- ✔ Independent Researchers
- ✔ Education

Roles

- ✔ Vulnerability Researchers
- ✔ Mobile Forensics



Why Choose Corellium for Mobile Vulnerability Research



Spin-Up Needed Devices

Easily access near limitless combinations of device models and iOS and Android, from past models and releases to the very latest.



Jailbreak and Root Access

Corellium can root any device configuration, including the latest version of iOS, even when no public jailbreak is available.



Low-Level Debugging

Leverage built-in kernel, iBoot, and SEP debugger tools for unprecedented introspection that can't be performed on physical devices.



Hypervisor Hooks

Dynamically patch the kernel with a performant C-like language to modify runtime behavior, trigger breakpoints from user-space, log function arguments, and more.



Matrix Testing

Script and automate vulnerability testing on multiple OS versions and device models simultaneously.



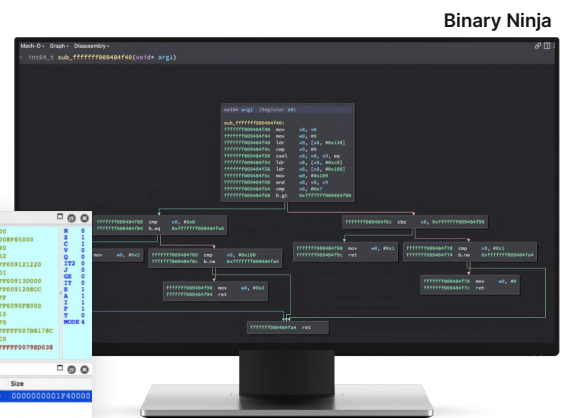
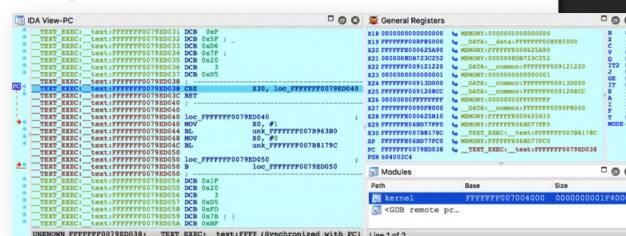
Comprehensive Integrations

Leverage the API and USBFlux to integrate with common tools, such as Xcode, Android Studio, IDA Pro, and GDB/LLDB.

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.

IDA Pro



Integrate with your favorites. Use side-by-side with your existing tools.



Technical Capabilities

Vulnerability Research

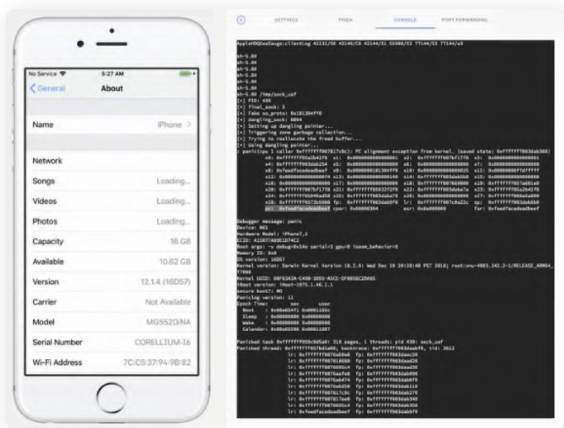
- ✔ Easily spin-up any combo of device, firmware, and mobile app
- ✔ Instantly jailbreak and gain root access, including the latest OS versions
- ✔ Supports kernel, iBoot, and SEP debugging
- ✔ Network traffic interception and tracing
- ✔ Built-in matrix testing and retrograding tests for older OS versions
- ✔ Research and test new and known exploits
- ✔ Practice weaponizing n-day iOS and Android exploits
- ✔ Experiment with new mitigations with live introspection and debugging (kernel and user-mode)

```
(lldb) reg wr x18 0x41414141
(lldb) reg read x18
x18 = 0x0000000041414141
```

```
(lldb) register read
General Purpose Registers:
x0 = 0x0000000000000000
x1 = 0x0000000000000001
x2 = 0x0000000000000000
x3 = 0xffffffff00001344
x4 = 0xffffffff00000010
x5 = 0xffffffff00000000
x6 = 0x0000000000000001
x7 = 0xffffffff00000000
x8 = 0x0000000000000000
x9 = 0x0000000000000000
x10 = 0x00000000ffffff33
x11 = 0x00000000ffffff33
x12 = 0x0000000000000000
x13 = 0xffffffff00001344
x14 = 0xffffffff00000000
x15 = 0x0000000000000000
x16 = 0xffffffff00001344
x17 = 0x0000000000000000
x18 = 0x0000000000000000
x19 = 0xffffffff00001344
x20 = 0x0000000000000000
x21 = 0x0000000000000000
x22 = 0xffffffff00001344
x23 = 0x0000000000000000
x24 = 0xffffffff00001344
x25 = 0xffffffff00001344
x26 = 0xffffffff00001344
x27 = 0x00000000ffffff33
x28 = 0x0000000000000000
x29 = 0xffffffff00001344
sp = 0xffffffff00001344
pc = 0xffffffff00001344
cpsr = 0x00000000
```

```
Process 1 stopped
* thread #1, stop reason = breakpoint 1.1
frame #0: 0xffffffff00718d6a4
-> 0xffffffff00718d6a4: ldr x8, [x8, #0x448]
0xffffffff00718d6a8: str xzr, [x8, #0x128]
0xffffffff00718d6ac: mrs x9, CNTCTL_EL0
0xffffffff00718d6b0: tbnz w9, #0x2, 0xffffffff00718d740
Target 0: (No executable module.) stopped.
(lldb)
```

Use standard debugging tools such as LLDB.



Trigger real 0-day and n-day vulnerabilities.

Training & Education

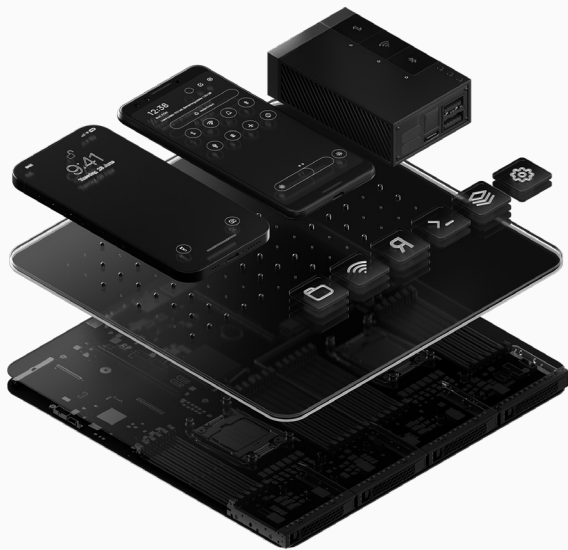
- ✔ Teach mobile security and testing best practices
- ✔ Vulnerability and exploit research training
- ✔ Inject artificial vulnerabilities for training
- ✔ Perform capture-the-flag (CTF) exercises

Compliance & Auditing

- ✔ Regulatory standards development, testing, and auditing
- ✔ Data privacy testing and auditing



Corellium Virtual Hardware Platform



VIRTUAL DEVICES

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

HYPERVERSOR

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.



Corellium Appliances

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



Corellium Cloud

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

Free trials at [Corellium.com](https://www.corellium.com)