Joe Grand's Hardware Hacking Advanced Training Course Agenda (NFI)

Last updated: February 4, 2026

Prerequisite: NFI's Hardware Hacking and Reverse Engineering Basic course

This two-day course focuses on advanced hardware hacking tools and techniques beneficial for digital forensic investigators. It is a hands-on environment where students will access and exploit various real-world hardware products. Each section contains an overview, examples, and hands-on exercises.

A. Firmware Extraction

- Locate debug interface of a Linux device using the JTAGulator
- Extract memory contents through JTAG, UART/bootloader, and device programmer

B. Firmware Modification

- Locate debug interface of a custom circuit board using manual methods
- Extract firmware with vendor-specific tools
- Reverse engineer firmware to identify security mechanism
- Modify and inject new firmware to bypass security

C. Side Channel Attacks

- Defeat PIN protection of a custom circuit board and external hard drive through timing leakage

D. Fault Injection

- Extract program code from a protected microcontroller using the ChipWhisperer

E. Open Lab/Case-Specific Projects