# VCA-RE-101 — Reverse Engineering of Embedded Systems

**Virtus Academy · Embedded Systems Reverse Engineering Stream**

## At a Glance

11 weeks · 4.0 units-equivalent · synchronous lecture + proctored laboratory Graduate-register · individual laboratory work · capstone with written report and oral defense

## Course Description

A laboratory-intensive course teaching the complete methodology for recovering design information, firmware, and cryptographic material from commercial embedded systems — without access to vendor source, schematics, or documentation. Students progress from physical-layer PCB characterization, through serial-protocol and debug-interface analysis (SPI, I²C, UART, JTAG, SWD), to SoC boot-sequence recovery, firmware extraction, binary reverse engineering, patch-and-reflash, and the trust architectures that defend against these techniques. The capstone is an end-to-end reverse engineering of a real commercial cable modem (Motorola SURFboard SB6141) delivered as a peer-review-quality written report and oral defense. The course is appropriate preparation for offensive security research, defensive firmware assurance, hardware-trojan analysis, supply-chain integrity evaluation, and forensic device examination.

## Learning Outcomes

On completion, graduates are able to:

1. Characterize an unknown printed circuit board by systematic physical measurement.
2. Identify SPI, I²C, UART, JTAG, and SWD protocols from observed bus waveforms.
3. Discover undocumented on-chip debug interfaces and verify discovered pinouts through independent methods.
4. Extract firmware from serial non-volatile memory using industry-standard programmers, with redundant-read cryptographic verification.
5. Analyze firmware images using binwalk, Ghidra, radare2, and QEMU.
6. Describe secure-boot and root-of-trust architectures, their threat models, and their practical attack surface.
7. Modify and reflash firmware to a target device while preserving recoverability to factory state.
8. Produce publication-quality technical reports suitable for USENIX Security, IEEE S&P, DEFCON, or coordinated-disclosure submission.

## Schedule

| Week | Topic | Laboratory |
|---|---|---|
| 1 | Foundations, threat models, laboratory setup | Bench qualification |
| 2 | Digital I/O, signal integrity, measurement | Logic analyzer fundamentals |
| 3 | Serial protocols: SPI, I²C, UART | Bus Pirate protocol exercises |
| 4 | JTAG and SWD | JTAG pinout discovery |
| 5 | SoC boot architectures and memory hierarchy | Boot sequence analysis |
| 6 | Non-volatile memory: NOR, NAND, eMMC | **Midterm practical exam** |
| 7 | Firmware extraction: in-circuit and ex-circuit | SB6141 flash dump |
| 8 | Firmware analysis: filesystems and signatures | SB6141 binwalk and extraction |
| 9 | Firmware analysis: executable reverse engineering | SB6141 binary analysis |
| 10 | Firmware modification and reflash | SB6141 patched firmware deployment |
| 11 | Trust architectures, secure boot, ethics | Live-device sniffing |

Capstone oral defenses are held in Finals Week.

## Assessment and Credential

Eleven laboratory exercises **55%** · midterm practical exam Week 6 **15%** · capstone written report **20%** · capstone oral defense **10%**. A minimum grade of B− on capstone components is required to earn the **VCA-RE-101 Certificate of Completion**. The program is independent; no affiliation with, or endorsement by, any government academy or university is claimed or implied.