The Full ROM Extraction Training
From Lab (ESP32) to Binary (Any Target)
// 4-days Session //
- Training Syllabus -

In an era where software security has reached its limits, the ultimate truth often lies within the hardware. Inside a chip, the ROM is usually the first vault worth breaking into: it stores cryptographic material, boot code, and hidden programming or test modes. This intermediate program addresses critical stakes in **Digital Forensics** (mobile evidence and crypto-wallet data extraction), S**upply Chain Verification** (backdoor research), **Hardware Security Evaluation**, and **IC Obsolescence Management**.

1. SUMMARY

The primary goal of this training is to provide security professionals and team leaders the skills, mindset and background information necessary to successfully perform the **reverse-engineering of Integrated Circuits** (ICs), circumvent their **hardware countermeasures** and **extract the data** from them (Hardware and Firmware).

This intermediate training is focused on **ROM memories,** as they are often the primary target of a security analysis at the transistor level. While the lab section takes the ESP32 as an example, the theoretical section is designed to learn ROMs independently of their type and embedded security measures.
As ROM content is encoded physically, it is possible to take pictures of the bits and convert them into a proper **binary**. Chip vendors, however, use techniques such as data scrambling and encryption to make these optical dumps impractical.
This training gives a complete understanding of how ROMs are constructed at the transistor level and shows how analyzing the circuitry can reveal the scrambling information necessary to reconstruct a proper binary.

Therefore, it is divided in two main sections :

- The first part of the training will be focused on the **extraction methods themselves**. This theoretical section aims at covering various ROMs from unencrypted to scrambled to fully protected versions, and consists in extracting a ROM from pictures only, working from Scanning Electron Microscope (SEM) images and following a step-by-step approach to extract a binary using Python, Fiji (ImageJ), Photoshop, and HDL (Hardware Description Language) tools.
- The second part will take place in “Le Lab” where an **ESP32** will be taken as an example case study. Sample preparation will be performed so as to identify the **ESP32 ROM** and its encoding layer, and covers ROM types, bit encoding, and ROM circuitry (logic, row and column decoders).

At the end of the session, attendees will be familiar with ROM technologies and able to adapt the acquired knowledge to real-life scenarios.

2. OBJECTIVES

Without being fully exhaustive, the key learning objectives of the training are to:

- Perform the sample preparation necessary to identify blocs of interest on an IC

- Become familiar with lab techniques such as wet chemistry and SEM imagery

- Identify ROMs on pictures of an Integrated Circuit (ESP32)
- Understand the building blocs of a ROM
- Identify the ROM type
- Extract a raw binary from pictures using simple scripts
- Reverse-engineer standard cells and semi-custom cells
- Reverse-engineer control logic, row and column decoders to uncover internal scrambling
- Convert the raw binary into binary candidates using the most common scrambling schemes
- Obtain the binary of ROMs
- Understand how to strengthen ROM designs
- Etc.

The lab session will feature hands-on demonstrations using the **ESP32**, and participants are also welcome to bring their own chips.

3. DETAILED DESCRIPTION

ROMs embedded in ICs are attractive targets because they may store **cryptographic** material, **boot code**, and hidden modes such as programming or test features. Understanding ROM contents enables activities ranging from **extracting Flash** data from inaccessible boot modes to conducting non-, semi-, or fully invasive **security evaluations**. These techniques are relevant to d**igital forensics**, **security assessments**, and **offensive security**.

Because ROM data is physically encoded, its bits are directly observable. With tools such as a Scanning Electron Microscope, both memory contents and control circuitry can be imaged, allowing sensitive information to be extracted at relatively low cost.

This hands-on training provides a deep understanding of **ROM architectures** and **dumping techniques**. It combines lab demonstrations, theory with practice, covering the circuits involved in ROM reading and applying this knowledge to **real cases**. Participants will not only analyze but also will be introduced to sample preparation techniques in “Le Lab” which are involved in the first stages of the RE process. As such, sample preparation and SEM imagery will be shown on the **ESP32** to introduce the theoretical and practice chapters the best way possible.

The theoretical part covers ROM structures and types, bit encoding and scrambling, and reverse-engineering of standard and semi-custom cells.
The practical part focuses on locating ROMs in IC images, extracting bits from SEM images using Fiji and Python, identifying ROM types, reverse-engineering decoders and control logic, and building HDL models of the memory. A VHDL testbench is then used to simulate ROM behavior and dump its content regardless of scrambling.

The course is structured progressively to reflect a **reverse-engineering mindset**, enabling attendees to develop their own workflows for future projects. It also addresses the current state of IC security and countermeasures, benefiting both chip designers and system integrators when evaluating device security.

SUMMARY OF TOPICS COVERED DURING THE COURSE

=> LE LAB

Targeting the **ESP32**, live demonstrations will illustrate the sample preparation necessary to isolate and image a ROM prior to extraction:

- Depackaging
- Top metal and substrate sample preparation
- Backside sample preparation
- SEM imagery & ROM localization

=> ROM Theory & Extraction

Covering various types of ROM architectures, methods and tools for extracting a ROM based on SEM pictures will be presented and related assignments will be proposed:

- ROM types and technologies
- Bit encoding and internal scrambling schemes
- Standard cell and semi-custom cell reverse-engineering
- Row and column decoder / control logic analysis
- Raw binary extraction from SEM images using Fiji and Python
- HDL modeling and VHDL-based simulation to dump the binary (ModelSim, Quartus or any other simulation tool)
- Adapting the methodology to other ROM types

4. TARGET AUDIENCE

This program is designed for high-level technical profiles, including:

- **Digital forensics** specialists focused on embedded evidence extraction from secure devices
- **Security professionals** performing hardware security evaluation and vulnerability assessment
- **Government** operators working in investigative, intelligence, or high-assurance security contexts
- Law enforcement authorities (**LEAs**) involved in digital investigations and evidence recovery
- **Chip designers** working on integrated circuit architecture and embedded countermeasures
- **OEMs** selecting and integrating secure components into products and systems
- **System integrators** responsible for deploying and validating secure hardware solutions
- **Supply chain security analysts** focused on hardware trust and backdoor detection
- Engineers and **researchers** involved in IC obsolescence management and legacy component analysis
- **Practitioners** working on secure IC data extraction and analysis in operational environments

5. MINIMUM SOFTWARE TO INSTALL

To follow the training efficiently, attendees are asked to bring a laptop with the following software installed:

- Fiji or ImageJ
- Python development environment
- Photoshop (evaluation versions are fine)
- ModelSim and Quartus Lite or any other VHDL simulation tool

- All of these tools can be downloaded as open-source software or as demo / evaluation versions.

6. PREREQUISITE

Prior knowledge of micro-electronics is not mandatory. Attendees should nevertheless be familiar with Python scripting and have some knowledge or understanding of HDL language. The training assignment are designed using VHDL as it is closer to actual design than Verilog, but attendees with Verilog skills will have no difficulty adapting. To accommodate attendees with no prior HDL (Hardware Description Language) experience, assignments are provided with scripts and files containing blanks to fill in.
Designed to challenge even active chip designers, our trainings explore ICs strictly from a reverse-engineering angle.

7. WHY TEXPLAINED?

In a security landscape often dominated by software-layer patches, Texplained stands as a global authority at the physical silicon level. Choosing our trainings means learning from the architects of modern IC exploitation:

- In a security landscape often dominated by software-layer patches, Texplained stands as a **global authority at the physical silicon level**. Choosing our training means learning from the architects of modern IC exploitation.
- **Proven** Pedigree: We don't just teach theory; we operate one of the world's leading secure IC Analysis Labs. Our methodologies are born from real-world forensic investigations and high-stakes security audits.
- The **ChipJuice** Advantage: Learn from the creators of ChipJuice, the industry-leading toolchain for automated hardware design recovery. We bridge the gap between manual microscopic analysis and scalable, automated exploitation.
- **Mission-Critical Expertise**: Our team capitalizes on more than 21 years of experience in solving the unsolvable when it comes to secret data extraction. We specialize in the most potent, fully-invasive techniques — the Gold Standard of hardware RE.
- **Actionable Intelligence**: We don't just show you how to break a chip; we show you **how to use** those results to conduct high-stakes digital forensics, execute the replacement of obsolete Integrated Circuits, and successfully identify hidden hardware backdoors.
- **Adaptive Learning Curve**: Our training is uniquely structured to take both newcomers and veterans through a **progressive, "pirate-mindset" workflow**, ensuring you leave with the autonomy to lead your own RE projects.

8. YOUR TRAINER: OLIVIER THOMAS



Olivier's expertise in the silicon domain began at the helm of one of the world's most elite Integrated Circuit (IC) Analysis Labs. Under his leadership, the facility focused on the dual mission of securing next-generation silicon and engineering robust countermeasures for current devices to **neutralize piracy and counterfeiting threats**.
During this tenure, Olivier pioneered numerous innovative techniques for semi- and fully-invasive IC analysis. His deep mastery of Failure Analysis (FA) methodologies and specialized laboratory

equipment allows him to pinpoint and **access vulnerable logic** on even the most hardened target devices.

As an Expert in **offensive hardware security**, Olivier is redefining the limits of automated IC analysis. His methodologies transcend traditional low-complexity targets, scaling effectively to the most hardened Secure Elements.
Olivier is also the architect of **ChipJuice**, a cutting-edge software toolchain designed to efficiently recover hardware designs regardless of their architecture, technology node, or Standard Cell Library.
He is the co-founder and CTO at Texplained.

9. WHAT YOU GET

Participants will receive slide decks covering both theoretical concepts and practical exercises. Each hands-on session includes step-by-step guidance and partial solutions to support attendees unfamiliar with the specific programming languages.
An optical scan of the substrate layer of the **ESP32** will also be provided.

10. INFORMATION & PRICE

- **Format**: 4 days combining theoretical modules with a hands-on laboratory session — sample preparation and imaging are demonstrated on an **ESP32**
- **Price**: Available upon request via your dedicated quotation
- **Registration**: Confirmed upon receipt of a signed training agreement

Ready to uncover what is really hidden inside silicon?