Integrated Circuit Reverse-Engineering & Data Extraction with Lab Hands-On Session
// 4-Days Session //
- Training Syllabus -

In an era where software security has reached its limits, the ultimate truth lies within the hardware. This elite program propels you from semiconductor architecture to surgical data extraction, addressing critical modern 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

This training is built for impact: two days of **intensive theory and structured exercises**, plus two days of immersive, **hands-on laboratory** session where everything comes alive in practice.

The applications are both critical and far-reaching—ranging from supply chain verification and hardware backdoor detection, to digital forensics and **evidence extraction from smartphones and crypto wallets**, IC obsolescence management, and hardware security evaluation. It is therefore highly relevant for professionals in **government agencies**, law enforcement authorities (**LEAs**), **semiconductor** companies, **system integrators**, and **security**-focused industries.

A dedicated **laboratory phase** turns knowledge into capability. Participants discover advanced sample preparation techniques (CMP), cutting-edge imaging tools (Optical & **SEM**), and invasive analysis methods. Live demonstrations, including **micro-probing**, reveal how real-world data extraction is performed and what it exposes about device security.

The course delivers a complete end-to-end understanding of the reverse-engineering and exploit chain—showing how modern integrated circuits behave under scrutiny and where their defenses break down. Participants learn how to exploit intrinsic weaknesses to recover critical assets such as **Netlists** and highly protected **NVM binaries**, using techniques typically reserved for advanced research environments.

By the end of the program, attendees will master key classes of high-end hardware attacks, including **bypassing shielding** and hardware **countermeasures**, **ROM and Flash/EEPROM dumping**, circuit **imaging**, and both passive and active **bus probing**.

More than a training, this is a structured pathway into **real-world hardware exploitation** and evaluation—designed to sharpen technical intuition, strengthen defensive thinking, and build practical reverse-engineering capability from the ground up.

2. OBJECTIVES

When working with secured or encrypted devices, several distinct objectives may arise: extracting embedded evidence, identifying potential hardware backdoors, detecting intrinsic vulnerabilities within a component that could be exploited by an attacker, or supporting IC obsolescence

management through the recovery and understanding of information from legacy components that are no longer documented or supported.

The primary goal of this training is to equip **digital forensics specialists**, **security professionals**, and **government agencies** with the skills, mindset, and foundational knowledge required to:

- **Recover the internal architecture** of integrated circuits (ICs)
- Extract non-volatile memory (**NVM**) contents, including ROM and Flash, to access and **retrieve sensitive embedded data**
- Evaluate the **effectiveness** of existing **hardware countermeasures**

Participants will also learn how these capabilities can be used to better understand and exploit hardware-level weaknesses, both for **vulnerability assessment** and for the r**ecovery of embedded evidence**.

Concretely, by the end of the course, participants will be able to:

- Perform low-level **hardware reverse engineering**
- Develop structured analysis strategies for target devices and apply them to **recover embedded data**
- Understand and apply laboratory techniques used for **netlist reconstruction** and **secure IC data extraction**

3. DESCRIPTION

Physical tampering techniques are typically grouped into three progressive families:

- Non-invasive methods such as clock and **VCC glitching** or **side-channel analysis**;
- Semi-invasive techniques including laser fault injection (**LFI**) and photo-emission analysis (**EMFI**);
- Fully invasive approaches that rely on advanced laboratory infrastructure such as deprocessing tools, Scanning Electron Microscopes (**SEM**), and Focused Ion Beam (**FIB**) systems.

At the highest level, fully invasive techniques are the **most powerful**. They provide direct access to the **internal structure** of a device and often reveal enough architectural detail to **unlock simpler** non- or semi-invasive **exploitation** paths by exposing the true weaknesses of both hardware and embedded implementations.

This training is designed for digital forensics specialists, security professionals, government agencies, and other stakeholders operating on **high-trust or high-security devices**. It delivers a complete understanding of the reverse-engineering and exploitation chain, enabling participants to gather **deep understanding** of secure systems across digital forensics, supply chain verification, IC obsolescence management, and hardware security evaluation by **identifying weaknesses** in secure elements for both **investigative and operational use cases**.

Participants are also introduced to non- and semi-invasive techniques, ensuring they can fully contextualize and exploit the results obtained through advanced hardware reverse engineering and data extraction workflows.

The program blends **theory** with **practice** in a highly applied format. Over **two intensive days at Texplained's laboratory**, participants move from concepts to demonstration, directly on real ICs and experiencing the full reverse engineering pipeline in a controlled and realistic environment.

The hands-on sessions are structured as a **progressive deep dive** into integrated circuits and the methods used to access embedded firmware and hidden data within secure ICs. Each step is designed to mirror a **true reverse-engineering mindset**, helping participants naturally develop their own workflows, strategies, and analytical approaches for future real-world engagements.

By the end of the training, participants will be able to design and execute low-level physical strategies involving reverse engineering, circuit analysis, and micro-probing. Non- and semi-invasive methods are also integrated throughout, as they often complement invasive findings to form practical, **efficient exploitation strategies** that do not always require full laboratory setups.

Finally, the course offers a rare, **up-to-date perspective** on the state of integrated circuit security and **embedded countermeasures**—insights that are directly relevant both to **chip designers** aiming to build stronger protections and to **OEMs** and integrators making high-stakes component choices, and to practitioners seeking to extract data from secure ICs in **digital forensics**, **supply chain verification**, and related investigative contexts.

Summary of topics covered during the course

=> Integrated Circuits Structure

- **Transistors, CMOS logic** and associated weaknesses
- Digital logic and Memories
- Failure Analysis and **Reverse-Engineering Methods**
- Embedded Firmware and Secret Data Dump: **ROM & Flash Dump**
- Analytical and Invasive ROM Dumps
- **Linear Code Extraction** (LCE) Based Methods
- **Automating** the Entire Process
- How to use the RE and code extraction **results**
- Choosing the right **types of attacks** for a given study
- **Non-, semi- and fully invasive** attacks with a focus on the latter
- **RE based attacks**

=> Lab:

- **Depackaging**
- Top metal and substrate **sample preparation**
- **SEM** imagery
- **X-section** and Shallow Angle Polish (**SAP**)
- **Deprocessing**
- Wire **bonding**
- **Micro-probing**

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 agencies** operating 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

All assignments will be provided in printed form, along with training materials distributed as PDF files. No specific software installation is required for the course.

6. PRERIQUISITE

This training does not require any specific prerequisites. The objective is to bring all participants, regardless of their initial background, to an operational level in Integrated Circuit reverse engineering.
No prior electronics expertise is mandatory, as the course begins with the fundamentals of digital electronics. A basic understanding of microcontroller architecture and assembly language can be beneficial, but these concepts are also introduced and covered during the early theoretical sections of the training.

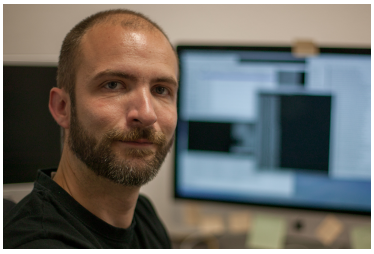
7. WHY TEXPLAINED?

In a security landscape often **dominated by software-layer patches**, Texplained stands as a global authority at the physical silicon level. Choosing our 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 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 went 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 THOMAS
Reverse Engineering Mentor

Oliver THOMAS studied Electrical Engineering (EE) and subsequently worked for a major semiconductor manufacturer designing analog circuits.

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.
A **pioneer in offensive hardware security**, Olivier is redefining the limits of automated IC analysis. His methodologies transcend traditional low-complexity targets like smartcards, scaling effectively to modern System-on-Chips (SoCs) featuring millions of gates and advanced technology nodes.
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. INFORMATION & PRICE

- **Format**: 4 days total (theoretical modules + 2 full days of hands-on laboratory sessions)
- **Material**: Comprehensive technical documentation provided in PDF format
- **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?