Factsheet 5: SiForensics

1. Introduction: The Role of SiForensics

The **ForRES project** (Forensic Reverse Engineering of Silicon chips) is a European initiative focused on advancing the field of **hardware-based digital forensics**, particularly aiming to advance the digital investigation to tackle cybercrime of electronic devices. As embedded systems become increasingly complex and security-critical, law enforcement agencies (LEAs), forensic analysts, and security researchers face growing challenges in extracting actionable intelligence from physical devices.

ForRES responds to this need by developing new methods, tools, and collaborative approaches for the **reverse engineering of ICs**, enabling the analysis of undocumented, tamper-resistant, or obfuscated hardware. Within this context, **SiForensics** plays a central role as the core software tool being developed in Work Package 3 (WP3). Its purpose is to convert raw physical data — including high-resolution micrographs of IC dies — into usable digital artifacts such as **gate-level netlists, ROM content, and structured design hierarchies**. This supports investigations where software-based forensics alone is insufficient or where hardware-based evidence is critical.

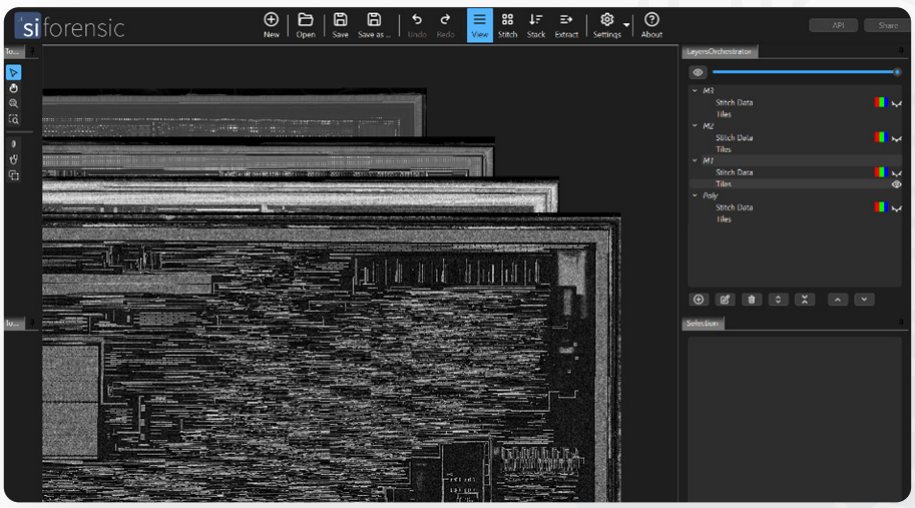
The development of SiForensics aligns closely with key objectives of the ForRES project. It aims to provide analysts with advanced capabilities for interpreting physical manifestations of circuit functionality, to enable the recovery of digital content from chip surfaces, and to foster collaboration across forensic teams. By bridging the gap between physical analysis and digital evidence generation, SiForensics strengthens the overall forensic capability and expands the scope of what is technically and legally accessible in cybercrime investigations. It is developed by law enforcement agencies for law enforcement agencies to support especially in the areas that are relevant for case work.

2. Functional Overview of SiForensics

SiForensics is ambitioned to be a modular, computer-aided reverse engineering (CARE) tool designed to facilitate the in-depth analysis of integrated circuits. Developed on the foundation of earlier software by the **BKA** (Germany's Federal Criminal Police Office), it is being significantly enhanced within ForRES to support a broader range of use cases and collaborative workflows.

The tool will provide a complete pipeline for chip analysis: from **image processing and visualization**, through **semi-automated logic and ROM extraction**, to **collaborative annotation and sharing**. Analysts will eventually be able to import, align (stitch), and stack high-resolution images of chip layers, view and annotate structures within the chip, and begin the process of identifying circuit elements and memory blocks. Using algorithmic and machine learning approaches, SiForensics assists in **detecting circuit tracks, vias, gates, and memory elements**, and will ultimately enable the **extraction of netlists** — digital representations of the chip's logic structure.

Beyond technical analysis, SiForensics will also be able to support the organizational aspect of forensic work, including a **collaborative interface**, allowing multiple analysts or institutions to contribute to the analysis of the same device, share findings, and co-develop conclusions. This is especially valuable in cross-border investigations or in cases where expert knowledge must be pooled across domains.



3. Development Structure and Core Tasks

The development of SiForensics is structured into three major tasks within WP3:

- **Semi-automated netlist extraction (T3.1):** Led by BKA, this task focuses on the semi-automated detection of circuit paths and the generation of digital netlists. It enables analysts to reconstruct the functional architecture of a chip from visual data.
- **ROM extraction support tools (T3.2):** Led by CSIC, this task develops tools to extract and interpret ROM content embedded in chips. ROM content is often crucial for identifying firmware, embedded code, or authentication mechanisms.
- **Support for collaborative chip analysis (T3.3):** Also led by BKA, this task builds the infrastructure for collaborative forensic analysis. It ensures that SiForensics can be used simultaneously by multiple users or teams, maintaining data integrity and synchronization.

The outputs of these tasks feed directly into other parts of the ForRES workflow, particularly in WP4, where recovered data is further analysed and interpreted for investigative purposes.

4. Software Structure and Availability

SiForensics will be released in **two parts,** each with a distinct licensing model and intended user base.

The **first part**, covering core functionality, will be released as **open source** under the **LGPLv3 license**. It includes image import and visualization, manual annotation, layer navigation, and collaborative tools. This part is intended for use by academic institutions, independent researchers, and any third parties interested in building on the platform or contributing to its development. The use of the LGPL license ensures that while the core remains free and open, developers can integrate proprietary modules without needing to open their own source code.

The **second part** includes all modules related to **automated analysis**, such as algorithmic netlist extraction, ROM recovery, and other advanced or potentially sensitive features. This part will be **closed source,** shared only with project partners, LEAs, and carefully vetted non-partner entities. Distribution will be tightly controlled to prevent misuse of the technology — for example, by actors attempting to bypass hardware security protections.

Both parts will be maintained through separate code repositories. The open-source portion will likely be hosted in a public git repository, while the closed-source modules will be developed and distributed through private channels.

5. Conclusion

SiForensics will represent a major step forward in the forensic analysis of modern hardware. By translating physical silicon structures into actionable digital information, it empowers analysts to uncover critical evidence hidden within the chips that power everyday devices. Whether investigating cybercrime, intellectual property theft, or hardware tampering, SiForensics enables a deeper, more precise understanding of how electronic systems operate — and how they can be reverse engineered, ethically and effectively, in support of justice and security.

Bundeskriminalamt TECHNIKON Netherlands Forensic Institute Ministry of Justice and Security CSIC POLITIET KRIPOS

Consortium
5 Partners
5 Countries

Budget
€ 2.3 Million
90% EU-funded

Duration
30 Months
07/2023 - 12/2025

Funded by the European Union under grant agreement no. 101102622. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.