# EMvidence: A Framework for Digital Evidence Acquisition from IoT Devices through Electromagnetic Side-Channel Analysis

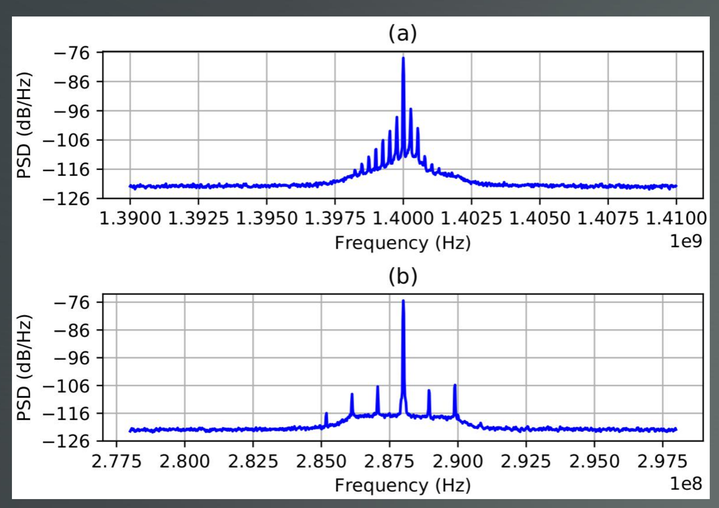
UCD Forensics and Security Research Group

**Asanka Sayakkara, Nhien-An Le-Khac, Mark Scanlon**
School of Computer Science, University College Dublin, Ireland.

## (1) The Challenge of IoT Forensics

- Internet of Things (IoT) devices are highly heterogeneous class of devices which are produced by different manufacturers with application-specific designs.
- The increasing use of IoT devices with limited standardisation makes it difficult to analyse them with traditional techniques.
- When encryption is involved, the task of IoT forensic investigation becomes even more challenging.
- Forensic tool developers are unable to provide tools which can collect forensic evidences from IoT devices due to this reason.
- The large variety of IoT devices in the market makes it virtually impossible to support all of them within a limited forensic tool set.

## (2) Electromagnetic Side-Channel Analysis



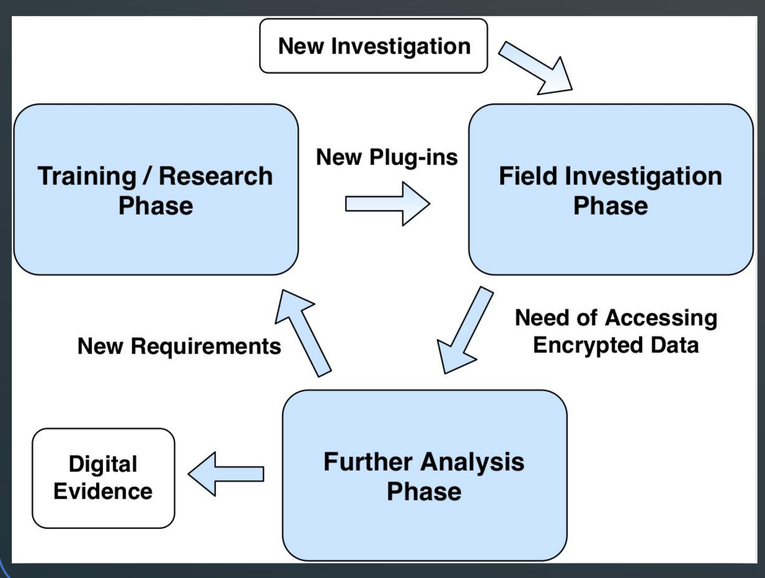

Leakage signals of two representative IoT devices
(a) Raspberry Pi 3 B+ at 1.4GHz
(b) Arduino Leonardo at 288MHz (18 th harmonic).

- Any time varying electric current can cause electromagnetic waves to radiate in to the space.
- Characteristics such as frequency and amplitude of EM waves depends on the characteristics of the EM source hence giving away some clues about the source.
- Different components on a computing device causes unintentional EM emission leaking different information.
- Different analysis methods such as SEMA and DEMA can help to extract information.

## (3) A Tool for EM-SCA in Digital Forensics

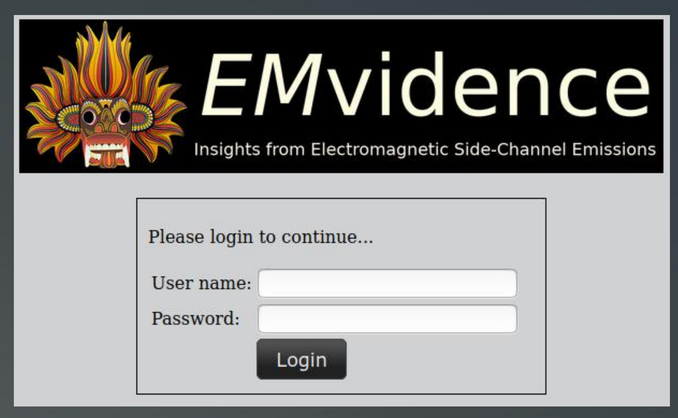
In order to gather forensically useful information using EM-SCA techniques, a software tool should facilitate three main phases.

1. Training/research phase where IoT devices and their forensically useful software activities are profiled and added into the framework.
2. Field investigation phase. where an investigator can collect EM data from a suspect IoT device in a real-world scenario and gather insights about the device on-the-spot.
3. Further analysis where the device is taken into a forensic laboratory and used to perform advanced EM-SCA methods such as cryptographic key recovery attacks.

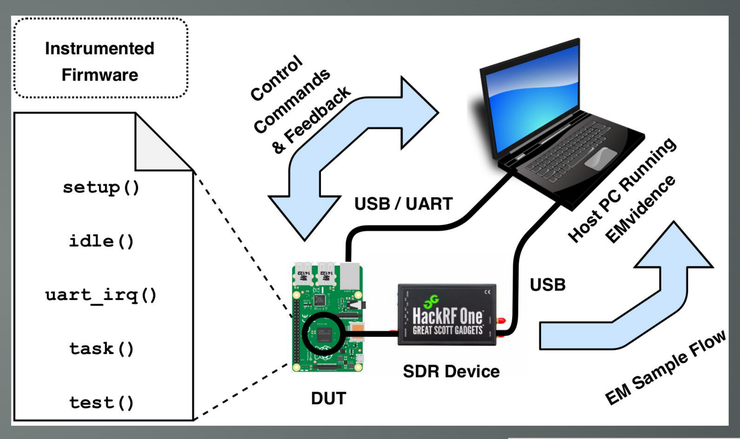



Three important phases a tool that facilitate EM-SCA in digital forensics should contain.

## (4) EMvidence Framework

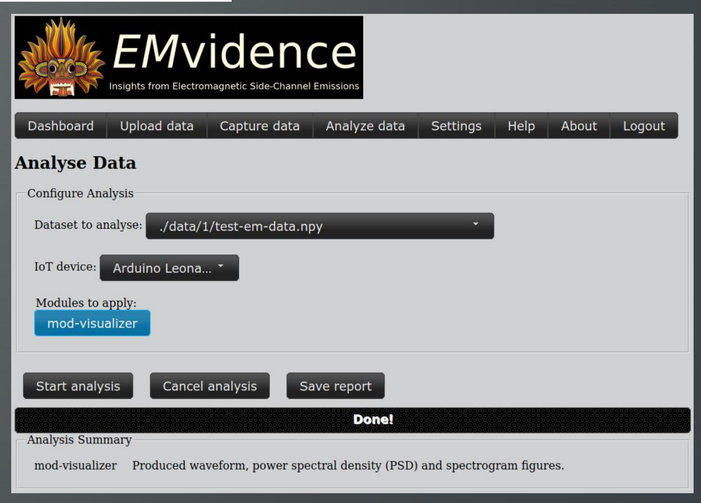


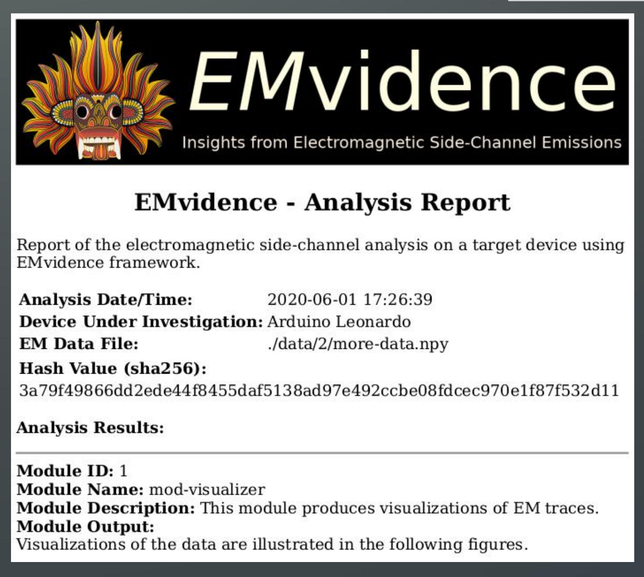

- EMvidence is an open-source framework that facilitate EM-SCA inspection of IoT devices.
- Main component of EMvidence is its core GUI that provides the default interface to a user. It also manages the modules and plug-ins by establishing communication between them in a coordinated fashion.
- EMvidence facilitates data acquisition, data visualisation and report generation.
- Depending on the requirements, third-party users can develop and add plug-ins to the core GUI of the EMvidence framework.
- Such plug-ins may provide various data analysis capabilities such as software behaviour detection, cryptographic key recovery, etc.




EM emissions of a target IoT device is captured through a software defined radio (SDR) directly with EMvidence.

Captured EM data can be analysed by applying various modules to the data.




Once the analysis is complete, a report is generated that illustrates the details of the data and results generated by different modules.

## (5) Future Direction

- EMvidence is currently undergoing constant development adding new features and fixing bugs.
- Lots of new features need to be added to make it fully usable in practical scenarios.
- You can help its development in various ways.

**Github Repository:**
https://github.com/asanka-code/EMvidence