Physical Analysis of Damaged IoT Devices

DFRWS EU 2022, Oxford

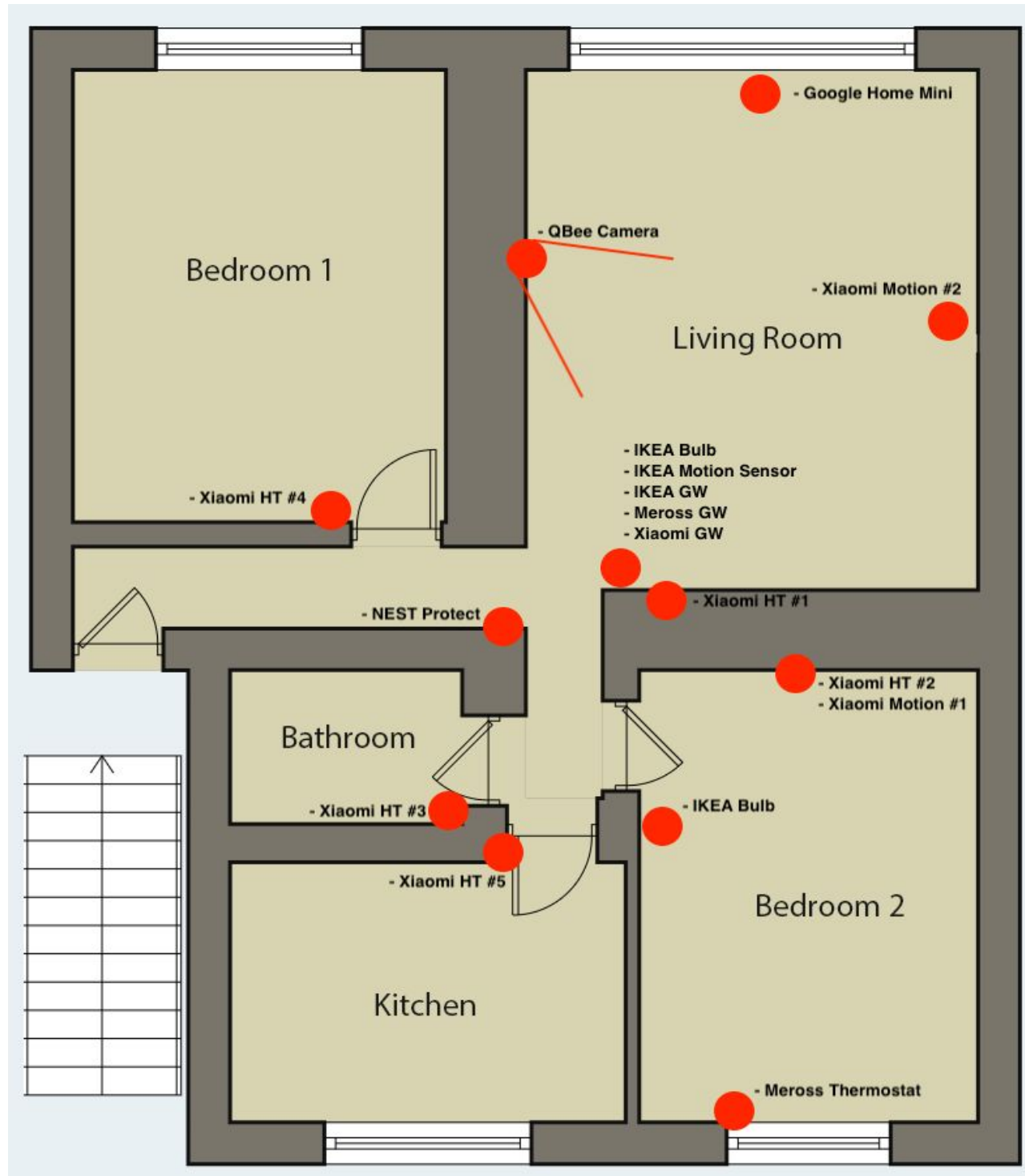Servida Francesco[1], Fischer Manon, Souvignet Thomas

Context

Fire Incident in Smarthome Environment

- **6 Ecosystems**
  - Ikea Trådfri
  - Xiaomi Mi Home
  - Google Home
  - Nest (Google)
  - Meross

- **1 Reference / Hub**
  - RPi with Home Assistant
    - Protected from fire

IoT Devices - Traces
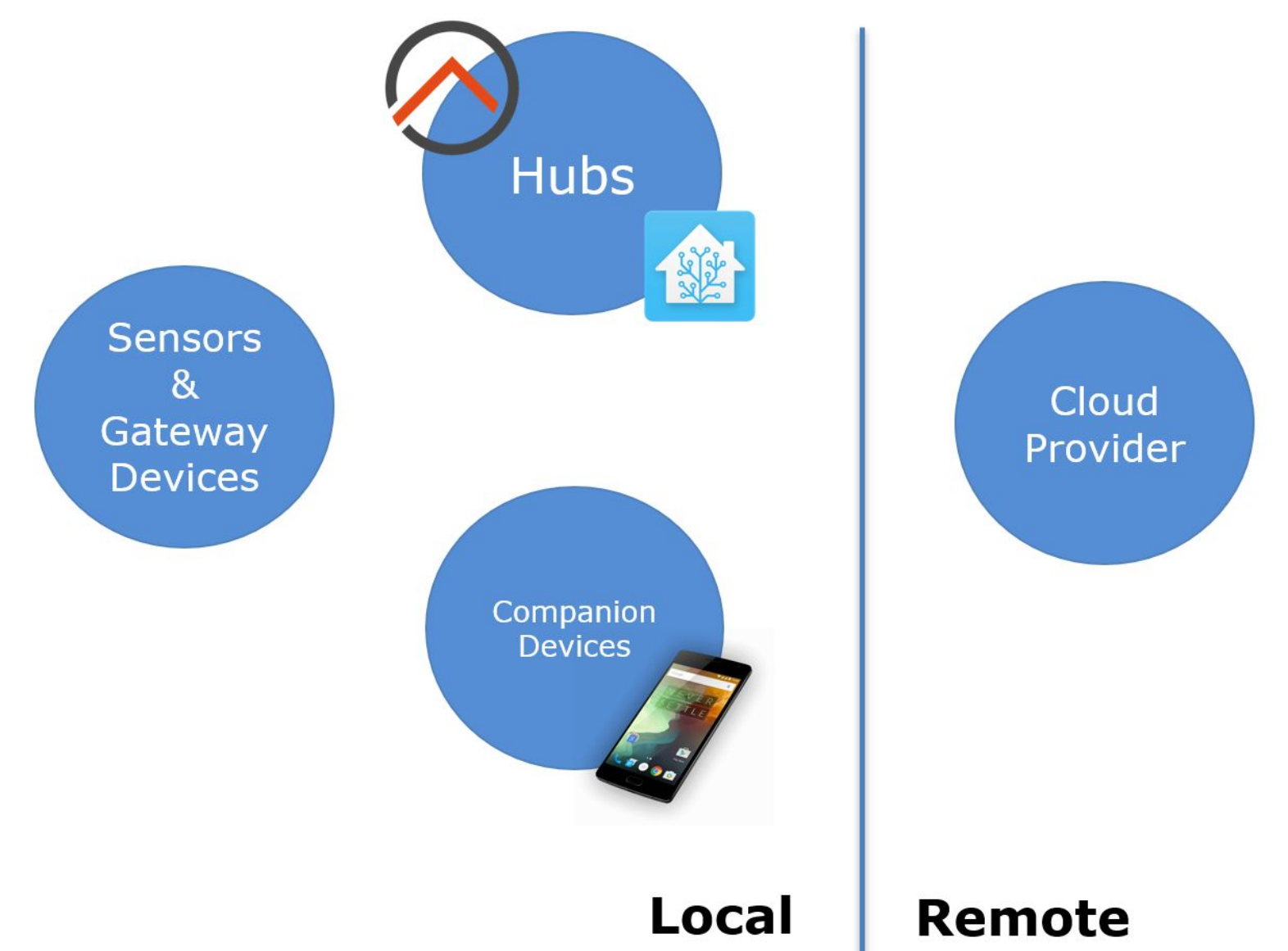
- **Chronology**
  - Detection of presence
  - Environmental conditions
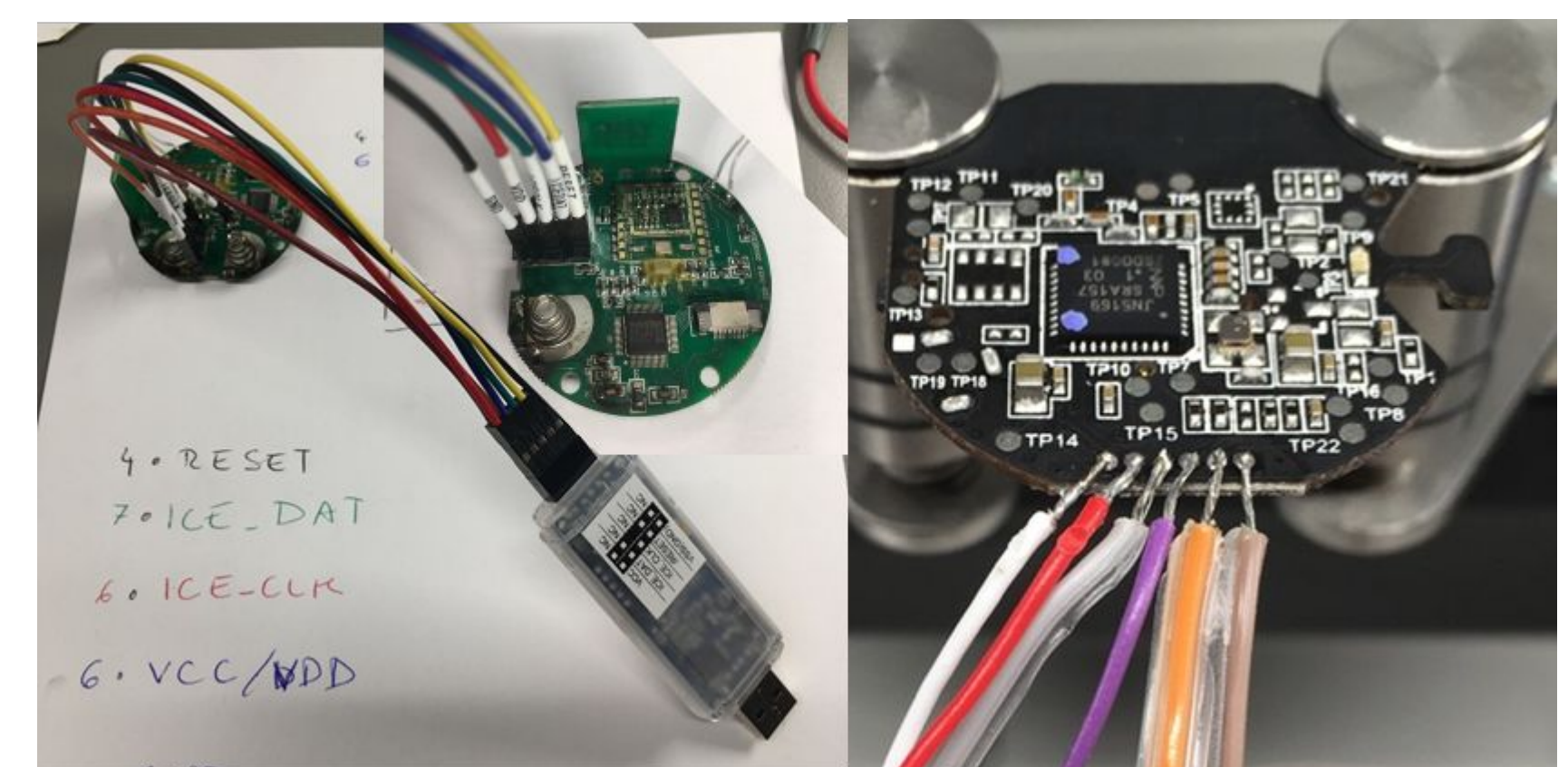 - Fire, Open Windows…

- **Identification**
  - Images/Voice Samples

- **Remote Credentials**
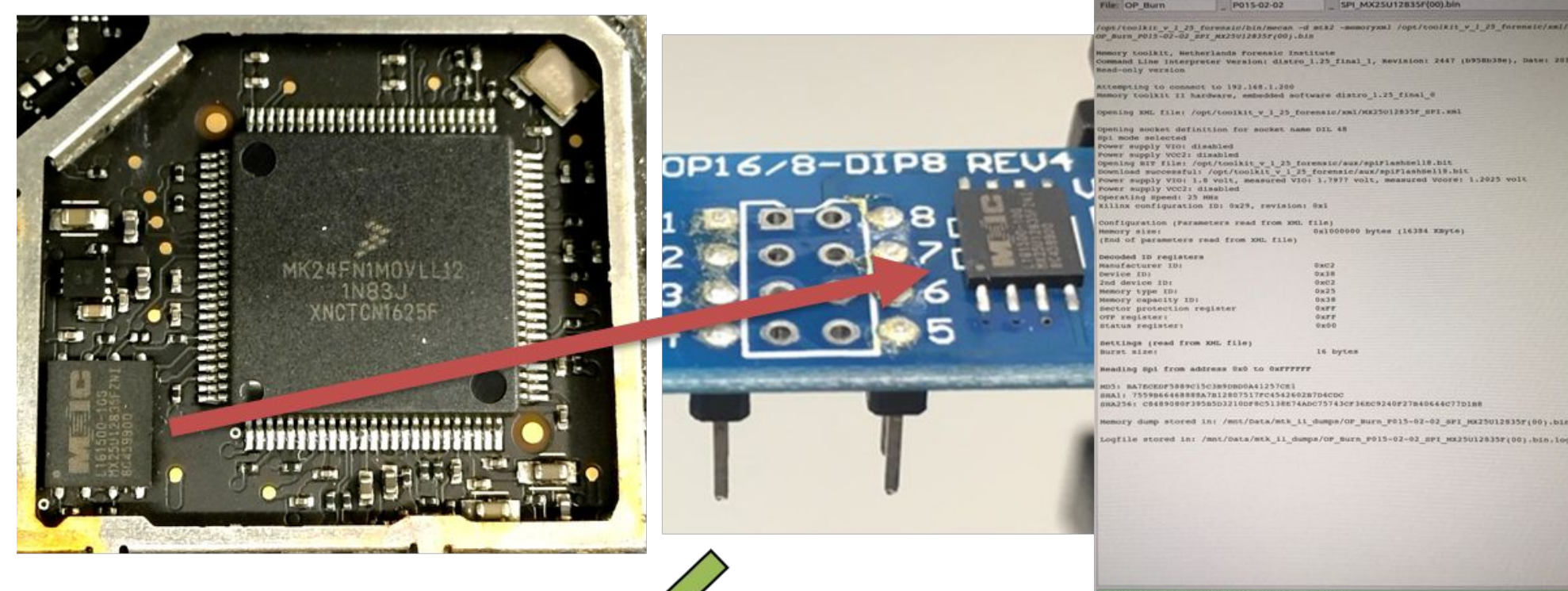- **Hints about other devices**

Local   Remote

Gateway and Sensors - Physical Analysis

Programming tools
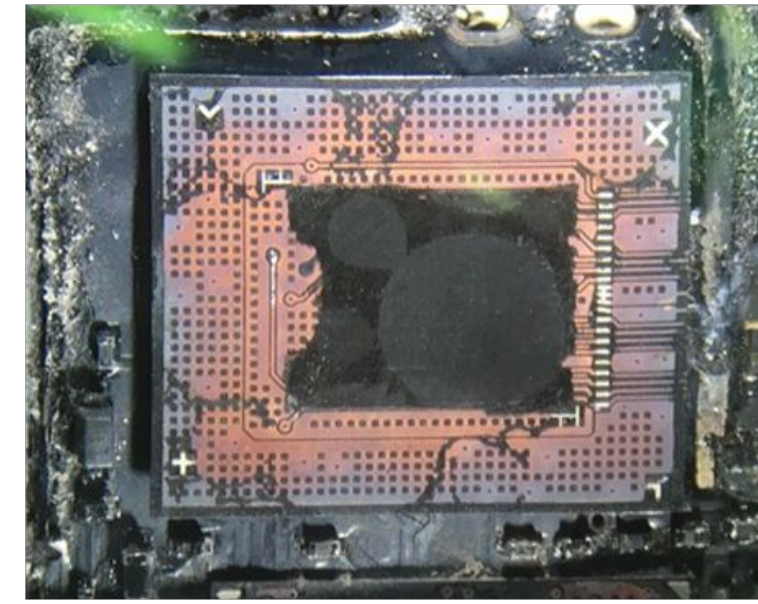- Still Functional Devices
- Memory embedded in SoC

Data Extraction

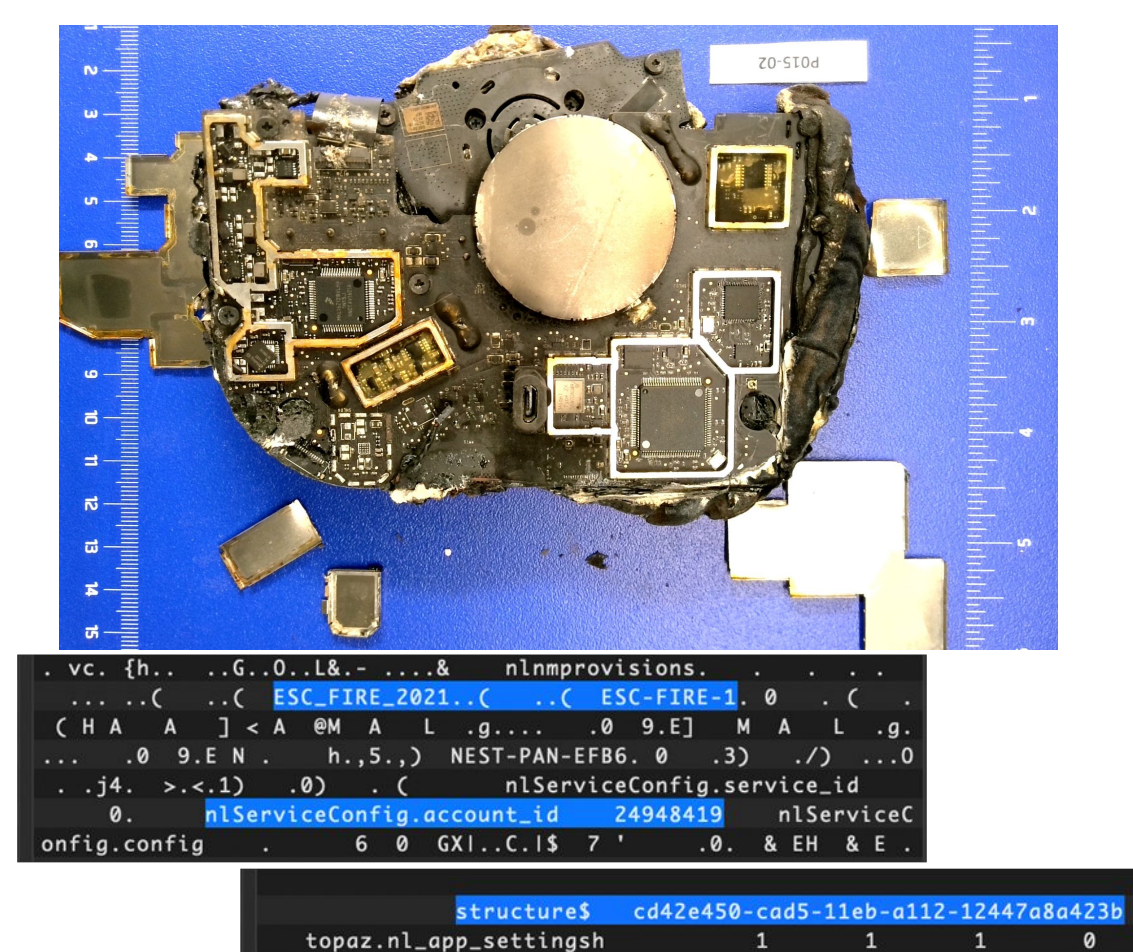**Chip Off** ✓

- Damaged devices
- Memory chips accessible

✗

Data Analysis

Qbee Camera

modelname=MOZART385s
SN=416B4067717

Nest Protect

Xiaomi Gateway

ssid="ESC-FIRE-1"
psk="ESC_FIRE_2021"
key_mgmt=WPA
uid=6463726721
6463726721
ctrl_interface=/var/run/wpa_supplicant
update_config=1
network={
    ssid="ESC-FIRE-1"
    scan_ssid=1
    psk="ESC_FIRE_2021"
    key_mgmt=WPA-PSK
    proto=WPA WPA2

LUMI_VERSION=3.3.10_116
SN=ZLMIGH1919007345
did=275958629
key=qVSrIXLSQ5ngDJLn
mac=50:EC:50:EE:63:F4
vendor=lumi
model=lumi.gateway.mieu01

Ikea Gateway

Meross	Google Home	Nest Protect	Xiaomi Home	Ikea Trådfri	QBee Camera
Thermostat & Gateway • No extraction possible	Damage to memory chips too extensive	• Account ID ☁ • Structure ID (Home ID?) ☁ • SSID and WiFi PSK	**Gateway** • Serial Number ☁ • Model ☁ • MAC Address ☁ • SSID and WiFi PSK • References to some sensors • BUT no evident logs Unable to reconstruct filesystem (**UBIFS**) due to memory corruption **Sensors** • No extraction possible	**Gateway** • Serial Number • Room Configuration • Device Configuration or Logs • No evident timestamped information **Lights** • No extraction possible	• Serial Number ☁ • Model ☁ • SSID and WiFi PSK

Cloud Provider - Traces
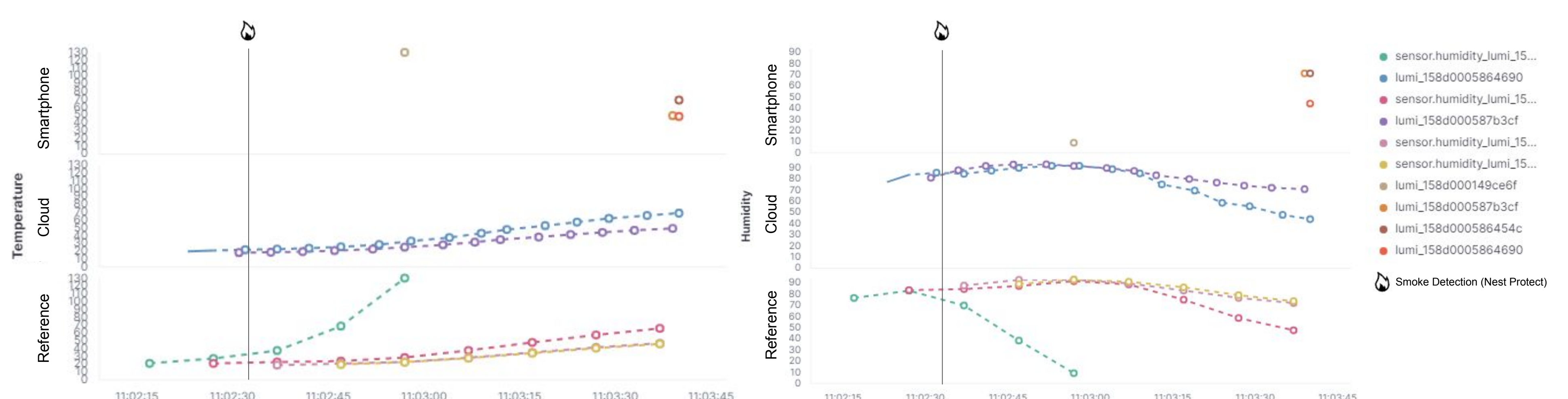
Future Research

- Most of the event data on cloud or smartphone
- IoT devices store information needed to identify them when requesting cloud data ☁

- Development of Knowledge Base storing:
  - What data is available
    - On the devices
    - On the smartphones
    - On the cloud
  - Data extraction techniques and decoders

- Allow sharing of information between services
- Prioritization of collection and analysis of IoT

- Servida, F. (2018). Internet of Things : Traces, Vulnerabilities and Forensic Challenges. MSc Thesis, University of Lausanne, Lausanne
- Servida, F., Casey, E. (2019). IoT Forensic Challenges and Opportunities for Digital Traces. Proceedings of DFRWS EU 2019
- Servida, F., Casey, E., Souvignet, T., Delémont, O., Bollé, T., Fischer, M. (2021). Enhancing Traditional Forensic Investigations using IoT Traces from Smart Buildings. Short Paper, DFRWS APAC 2021

[1] francesco.servida@unil.ch, School of Criminal Justice, University of Lausanne, Switzerland