SANS | GIAC CERTIFICATIONS

Home Automation and IoT as a Source of Evidence

Forensic Analysis of Home Assistant

ANDREA LAZZAROTTO

ANDREALAZZAROTTO.COM

About me

- Digital Forensics Consultant and Software Developer
- Interests include WhatsApp forensics and anti-forensics
- Author of several open-source tools, such as **RecuperaBit** for NTFS reconstruction and **Carbon14** for estimating the publication date of a web page (both included in CAINE)
- **Author of Fuji,** the new open source program for the forensic acquisition of macOS

Agenda

Introduction to Home Assistant

Open-source home automation system

Data analysis

Reading configuration files and the database

Practical examples

Answers you can obtain

SANS | GIAC CERTIFICATIONS

Introduction to Home Assistant

Open-source home automation system

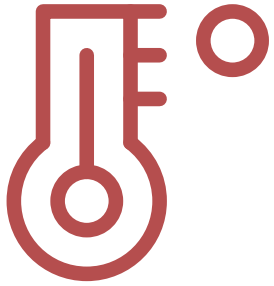
Home automation systems

IoT (Internet of Things) devices are everyday objects equipped with Internet connectivity, capable of collecting, transmitting, and exchanging data.

Home automation is based on the creation of integrated systems for the automation and management of various aspects of the home, such as heating, lighting, and security.

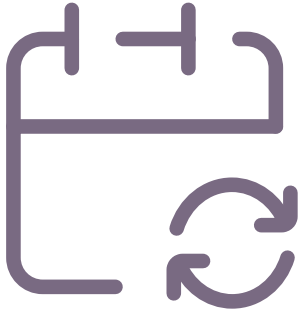
Home automation systems usually integrate IoT devices.

Reasons to analyze them



Numerous sensors

A “smart” home can be equipped with dozens or hundreds of sensors



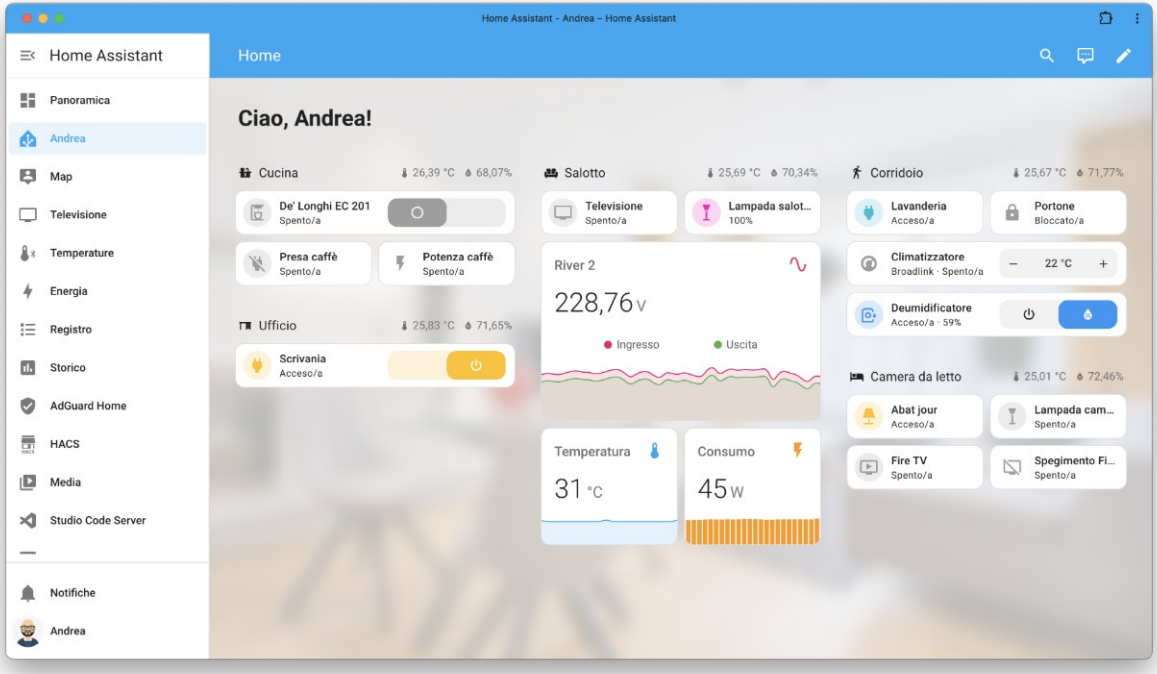
24/7 data flow

Data is continuously collected and the system is never turned off

User activity

From reading the status of sensors and actuators, we can infer human activity

Home Assistant



Home Assistant is an open-source home automation solution that integrates with several devices.

The *local* mode is preferred to protect user data, but it also supports multiple *cloud* integrations.

Devices and entities

Physical devices and any “virtual objects” connected to Home Assistant are classified as **devices.**

Each device can have various **entities,** which correspond to sensors and actuators.

Examples:

- Smart plug device with a status entity (on/off) and a power consumption sensor
- Plex server device with an entity that indicates the presence of a software update

Automations and scenarios

Devices (and their entities) can be activated using **automations** that are run when certain conditions are met.

Scenes represent a set of states that you want to activate simultaneously (for example, turning on three different entities at the same time).

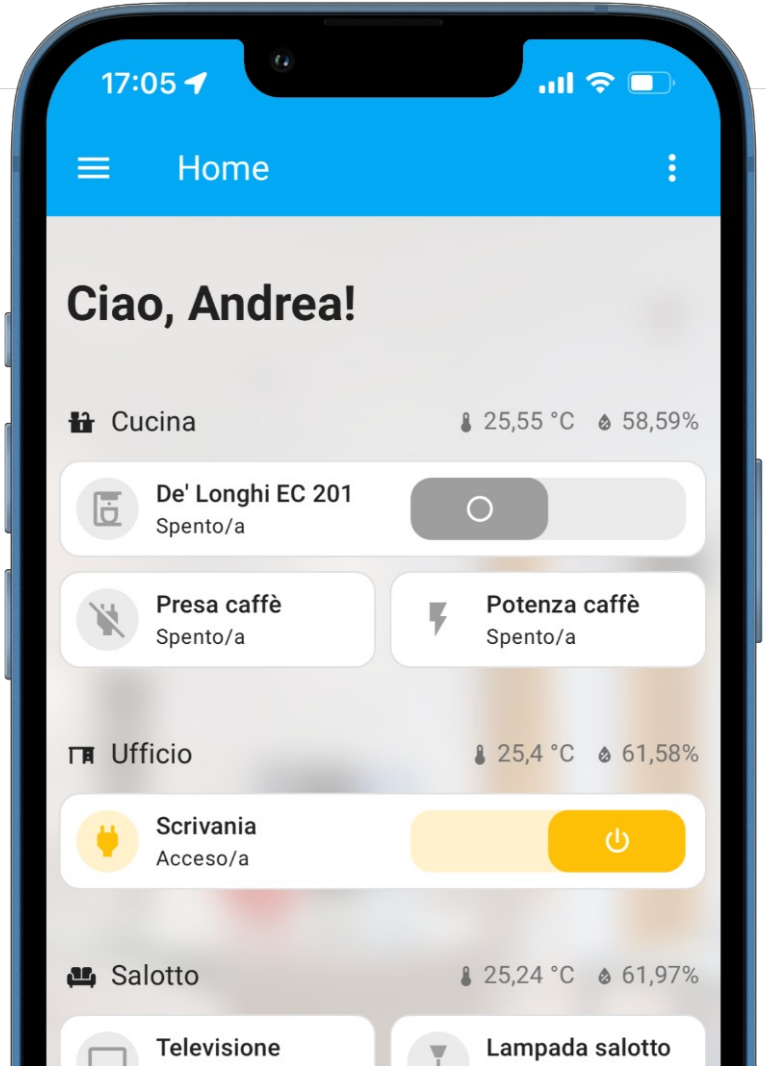
There are also **scripts,** which are actions that need to be executed in sequence.

Mobile app

Home Assistant provides an app for Android and iOS, allowing the user to control all devices remotely.

Additionally, **the app becomes a device** and adds various entities corresponding to phone sensors.

For example, Home Assistant reads and records the battery charge level.



SANS | GIAC CERTIFICATIONS

Data analysis

Reading configuration files and the database

Home Assistant OS

The Hass.io operating system is entirely based on Docker.

The disk partitioning consists of eight volumes, which basically contain system programs, files related to the kernel, or those pertaining the operation of containers.

The only partition we care about is hassos-data.

Data volume

Configuration files

Related to the platform supervisor

Add-ons

Potentially installed by the user

Historical database

Containing data records

Configuration files

The supervisor configurations are located in the main directory `/supervisor`, within several JSON files.

The `addons.json` file is of particular interest because it lists **official add-ons** that the user added to their installation.

The application configurations are mainly found in the file `/supervisor/homeassistant/configuration.yaml` and some other files in the same directory.

Add-ons

The relevant files for official add-ons are located in `/supervisor/addons` and `/supervisor/addon_config`.

Additionally, the user can manually add “custom” components, either via file upload or through the **HACS (Home Assistant Community Store).**

The latter are found in the `custom_components` directory contained in `/supervisor/homeassistant`.

History database

The **most important** file is `home-assistant_v2.db`, located in `/supervisor/homeassistant`.

It is an SQLite archive that stores what has occurred in the system: the history of events, state changes for non-numeric entities (*states*), and those for numeric entities (*statistics*).

Analyzing the history database with some SQL queries lets us **extract a vast amount of data.**

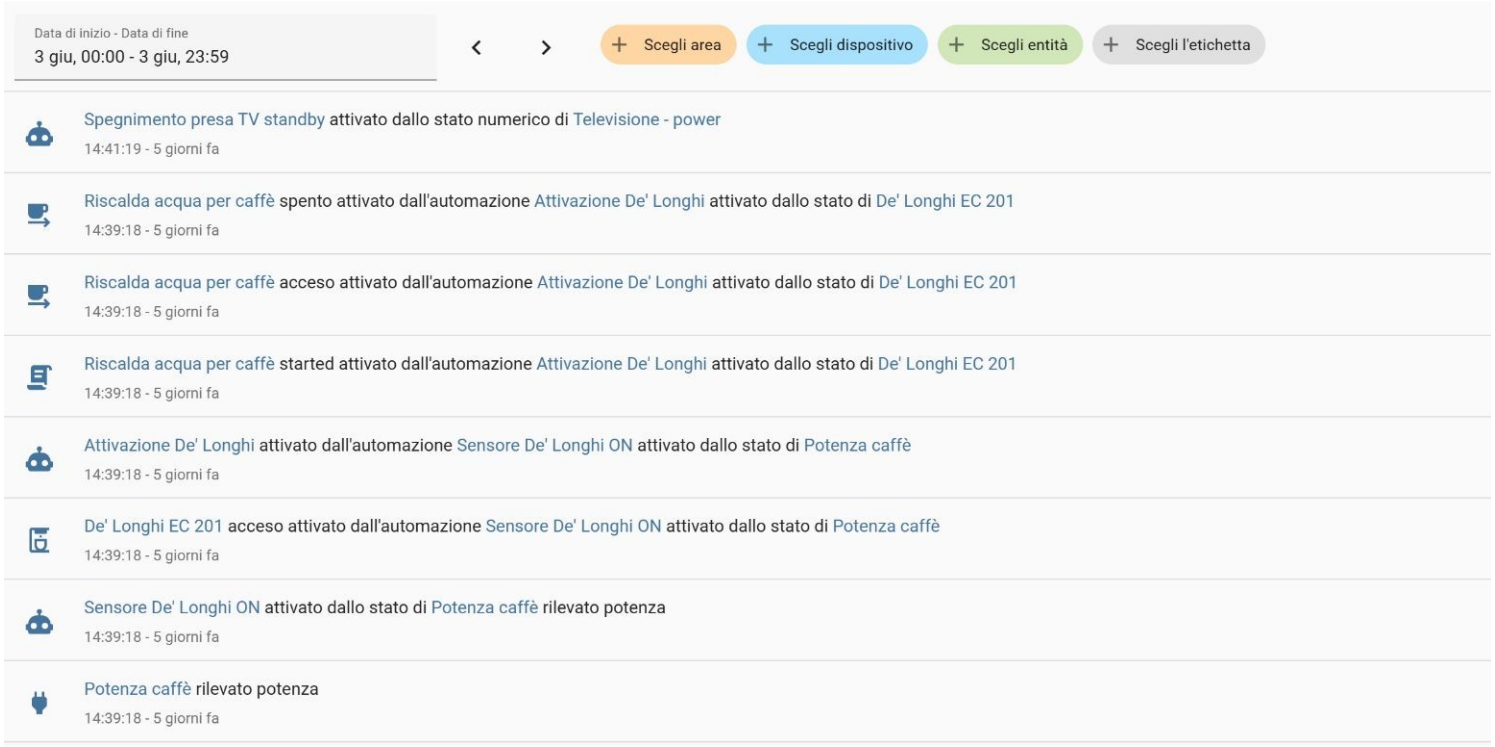
This database can also be obtained by exporting a backup from the web interface.

SANS | GIAC CERTIFICATIONS

Practical examples

Answers you can obtain

Device activations



Corresponding SQLite query

```
SELECT events.event_id, SUBSTR(HEX(events.context_id_bin), 25, 10) AS ctx,
SUBSTR(HEX(events.context_parent_id_bin), 25, 10) AS parent_ctx,
DATETIME("time_fired_ts", 'unixepoch', 'localtime') AS datetime,
shared_data ->> '$.entity_id' AS entity_id, […], event_data.*
FROM events JOIN event_data ON events.data_id = event_data.data_id
WHERE datetime LIKE '2025-06-03 %'
ORDER BY time_fired_ts DESC
```

	event_id	ctx	parent_ctx	datetime	entity_id	service	service_entity_id	name	
29	14199124	DE68B617	ED46EE8F	2025-06-03 14:41:19	NULL	turn_off	switch.televisione_outlet	NULL	NULL
30	14199123	DE68B617	ED46EE8F	2025-06-03 14:41:19	automation.spegnimento_presa_tv_sta…	NULL	NULL	Spegnimento presa TV standby	numeric sta
31	14199121	B5448A4E	842E7C4B	2025-06-03 14:39:18	NULL	turn_on	switch.macchina_caffe_outlet	NULL	NULL
32	14199120	B5448A4E	842E7C4B	2025-06-03 14:39:18	script.riscalda_acqua_per_caffe	NULL	NULL	Riscalda acqua per caffè	NULL
33	14199119	B5448A4E	842E7C4B	2025-06-03 14:39:18	NULL	riscalda_acqua_per_caffe	NULL	NULL	NULL
34	14199118	B5448A4E	842E7C4B	2025-06-03 14:39:18	automation.attivazione_de_longhi	NULL	NULL	Attivazione De' Longhi	state of …
35	14199117	842E7C4B	052BF7F0	2025-06-03 14:39:18	NULL	turn_on	["input_boolean.de_longhi_ec_201"]	NULL	NULL
36	14199116	842E7C4B	052BF7F0	2025-06-03 14:39:18	automation.de_longhi_on	NULL	NULL	Sensore De' Longhi ON	state of bi

Environmental sensors

Thanks to Home Assistant statistics, we can read the data coming from all sensors located in the home (logs are detailed for the first 10 days, then sampled hourly).

Examples:

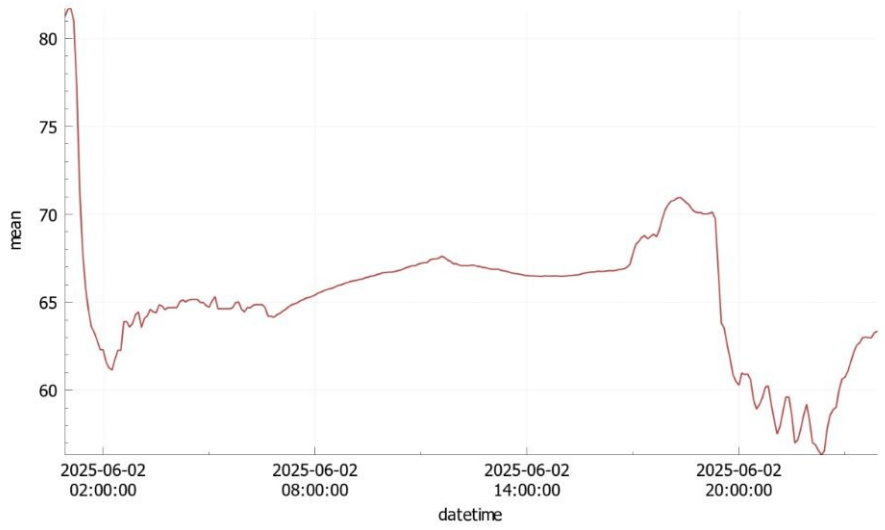
- A sudden drop in humidity in a specific room may indicate that a window has been opened
- A spike in humidity in the bathroom indicates the time of use of the shower
- A significant power consumption may indicate the use of an appliance like the washing machine

Generating the plot

Using DB Browser for SQLite, we can generate a plot for this query:

```
SELECT DATETIME("created_ts",
'unixepoch', 'localtime') AS datetime, *
FROM statistics_short_term
WHERE metadata_id = 38
AND datetime LIKE '2025-06-02 %'
ORDER BY datetime ASC
```

The value 38 for “bathroom humidity” was obtained from the `statistics_meta` table.



Our mobile phones have become the greatest spy on the planet.

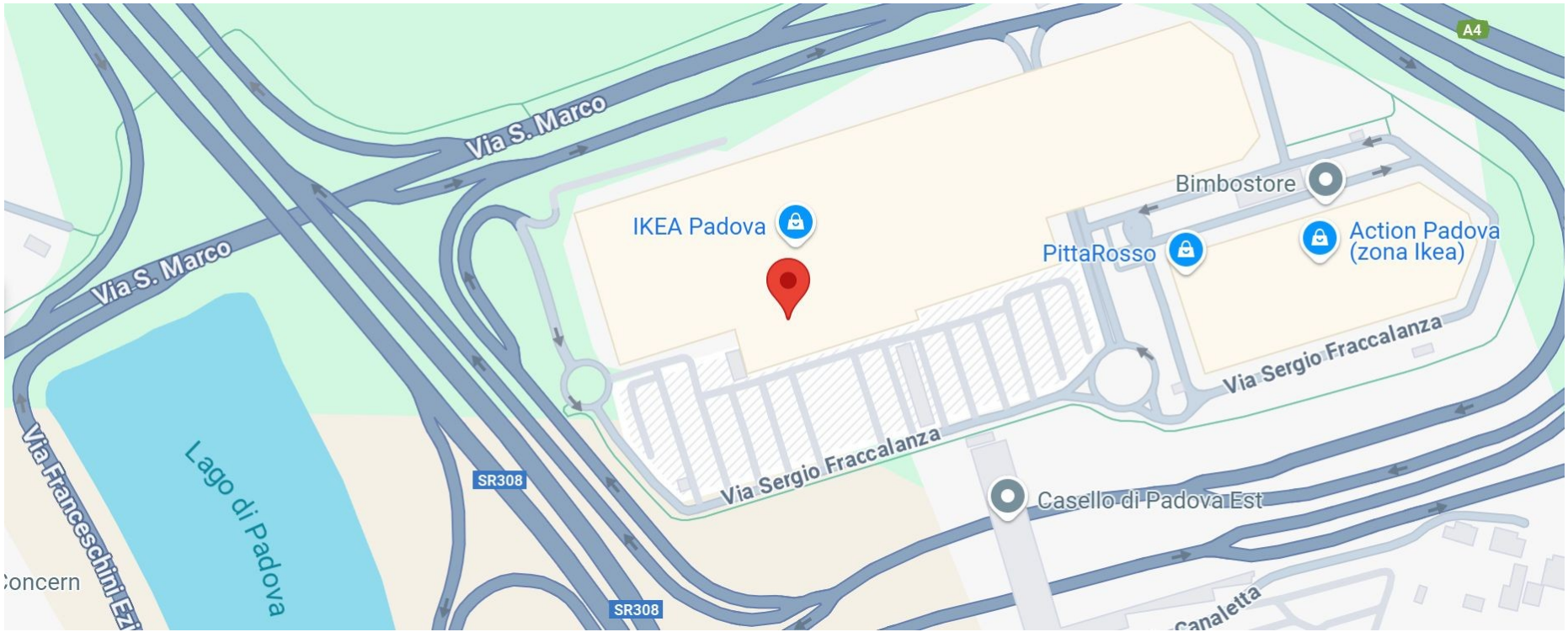
— JOHN MCAFEE

Locations recorded by the app

```
SELECT DATETIME("last_updated_ts", 'unixepoch', 'localtime') AS datetime,
shared_attrs ->> '$.latitude' AS latitude, shared_attrs ->> '$.longitude' AS
longitude, […], states_meta.entity_id, state_attributes.shared_attrs
FROM states_meta JOIN states ON states_meta.metadata_id = states.metadata_id
JOIN state_attributes ON states.attributes_id = state_attributes.attributes_id
WHERE (states_meta.entity_id LIKE 'device_tracker.%' OR states_meta.entity_id LIKE
'%geocoded_location') AND datetime LIKE '2025-06-01%'
```

	datetime	latitude	longitude	place	city	name	source	entity_id	s
20	2025-06-01 11:27:32	45.4172220632236	11.9245069775236	NULL	NULL	iPhone di Andrea	gps	device_tracker.iphone_di_andrea	{"source_type":
21	2025-06-01 11:27:32	NULL	NULL	Via San Marco 42	Padova	iPhone di Andrea Geocoded Location	NULL	sensor.iphone_di_andrea_geocoded_lo…	{"Administrativ
22	2025-06-01 11:37:20	NULL	NULL	Centro Commerciale Padova Est	Padova	iPhone di Andrea Geocoded Location	NULL	sensor.iphone_di_andrea_geocoded_lo…	{"Administrativ
23	2025-06-01 11:37:20	45.4186055977072	11.9327101400843	NULL	NULL	iPhone di Andrea	gps	device_tracker.iphone_di_andrea	{"source_type":
24	2025-06-01 20:53:02	45.421214357485	11.9273591609408	NULL	NULL	iPhone di Andrea	gps	device_tracker.iphone_di_andrea	{"source_type":
25	2025-06-01 20:53:02	NULL	NULL	Via Anna Maria Mozzoni 5-9	Padova	iPhone di Andrea Geocoded Location	NULL	sensor.iphone_di_andrea_geocoded_lo…	{"Administrativ

Result


A4
Via S. Marco
Via S. Marco
IKEA Padova
Bimbostore
PittaRosso
Action Padova
(zona Ikea)
Via Sergio Fraccalanza
Via Sergio Fraccalanza
Via Franceschini Ezi
Lago di Padova
SR308
SR308
Casello di Padova Est
oncern
Canaletta

SANS | GIAC CERTIFICATIONS

Thank you

Web
andrealazzarotto.com

GitHub
Lazza

X / Twitter
@thelazza

Mastodon
@lazza@mastodon.social