

A modern, minimalist living room with a light-colored sofa, a round coffee table, and a large television. A staircase is visible in the background. The image is overlaid with a semi-transparent white box containing text.

Domotica e IoT come fonte di prova

ANALISI FORENSE DI HOME ASSISTANT

ANDREA LAZZAROTTO

ANDREALAZZAROTTO.COM

A proposito di me

- Laurea magistrale in Informatica
- Consulente informatico forense e sviluppatore
- Attività di ricerca sulla *WhatsApp forensics* e *anti-forensics* (manipolazione delle chat) e l'acquisizione e analisi dei metadati dei profili Instagram
- Autore di alcuni strumenti open source, come **RecuperaBit** per la ricostruzione di NTFS e **Carbon14** per datare le pagine web (entrambi si trovano in CAINE)
- **Autore di Fuji**, il nuovo software open source per l'acquisizione forense dei computer con macOS



Agenda

INTRODUZIONE A HOME ASSISTANT

Sistema di domotica open source

ANALISI DEI DATI

Copia forense e lettura del database

ESEMPI PRATICI

Quali risposte è possibile ottenere

Introduzione a Home Assistant

SISTEMA DI DOMOTICA OPEN SOURCE

Sistemi domotici

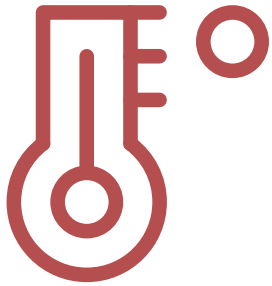
I dispositivi **IoT** (***Internet of Things***) sono oggetti di uso quotidiano dotati di connettività a Internet, capaci di raccogliere, trasmettere e scambiare dati.

La **domotica** si basa sulla creazione di sistemi integrati che permettono di automatizzare e gestire diversi aspetti della casa, come il riscaldamento, l'illuminazione e la sicurezza.

I sistemi domotici avanzati integrano anche dispositivi IoT.

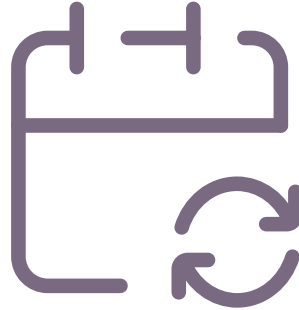


PERCHÉ ANALIZZARLI



Numerosi sensori

Una casa "intelligente" può essere dotata di decine o centinaia di sensori



Flusso di dati 24/7

I dati vengono raccolti continuamente, il sistema non viene mai spento



Attività dell'utente

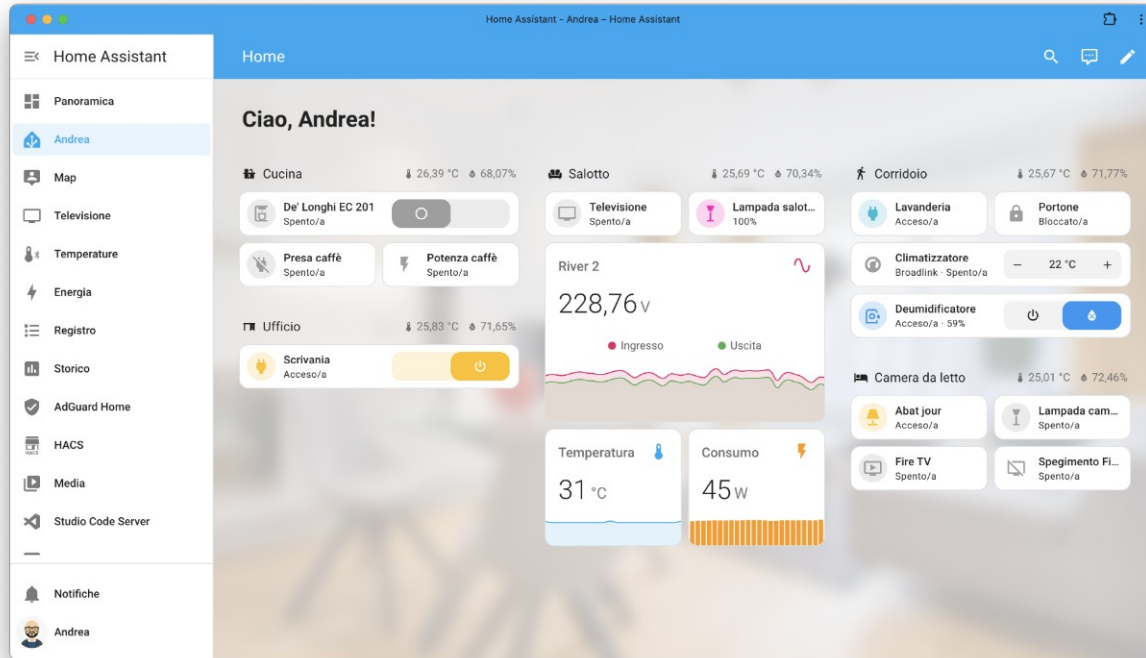
Dalla lettura dello stato di sensori e attuatori possiamo dedurre l'attività umana



The S in IoT stands for Security.

— TIM KADLEC

HOME ASSISTANT



Home Assistant è una soluzione domotica open source, che si integra con numerosi dispositivi.

Viene preferita la modalità *locale* per tutelare i propri dati, ma permette anche integrazioni *cloud*.

Tipi di installazione

HOME ASSISTANT OS (HASS.IO)

Sistema operativo dedicato con tutti i componenti

CONTAINER

Installazione all'interno della piattaforma Docker

ALTRI METODI

Le modalità *Supervised* e *Core* sono state deprecate



Dispositivi ed entità

Gli apparati fisici ed eventuali “oggetti virtuali” collegati a Home Assistant vengono classificati come **dispositivi**.

Ciascun dispositivo può possedere diverse **entità**, che corrispondono a sensori e attuatori.

Esempi:

- Dispositivo *smart plug* con entità di stato (acceso/spento) e sensore del consumo di potenza
- Dispositivo server Plex con entità che segnala la presenza di un aggiornamento software

Automazioni e scenari

I dispositivi (e le relative entità) possono essere azionati utilizzando delle **automazioni** che vengono eseguite al verificarsi di determinate condizioni.

Le **scene** rappresentano un insieme di stati che si desidera attivare nello stesso momento (per esempio accendendo tre diverse entità contemporaneamente).

Esistono anche gli **script**, cioè azioni che devono essere eseguite in sequenza.

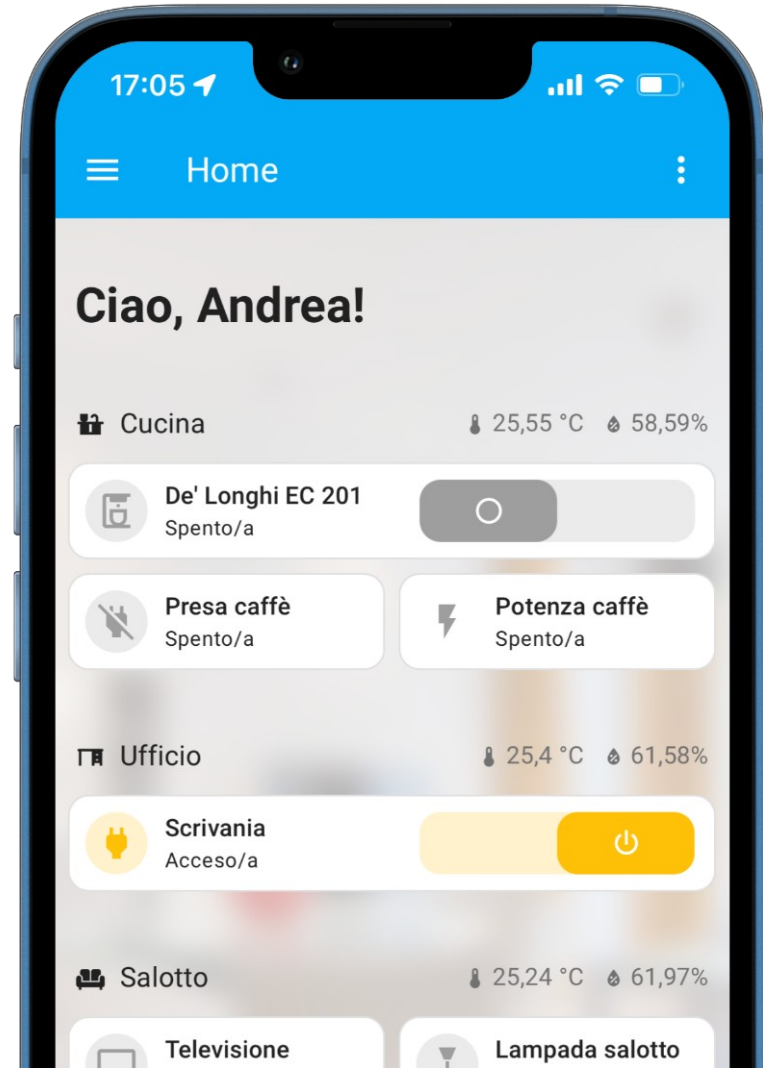


App per smartphone

Home Assistant fornisce un'app per Android e iOS, perciò l'utente può controllare tutti i dispositivi anche in modalità remota.

Inoltre **l'app diventa un dispositivo** e aggiunge varie entità che corrispondono a sensori del telefono.

Per esempio, Home Assistant legge e registra il livello di carica della batteria.



Analisi dei dati

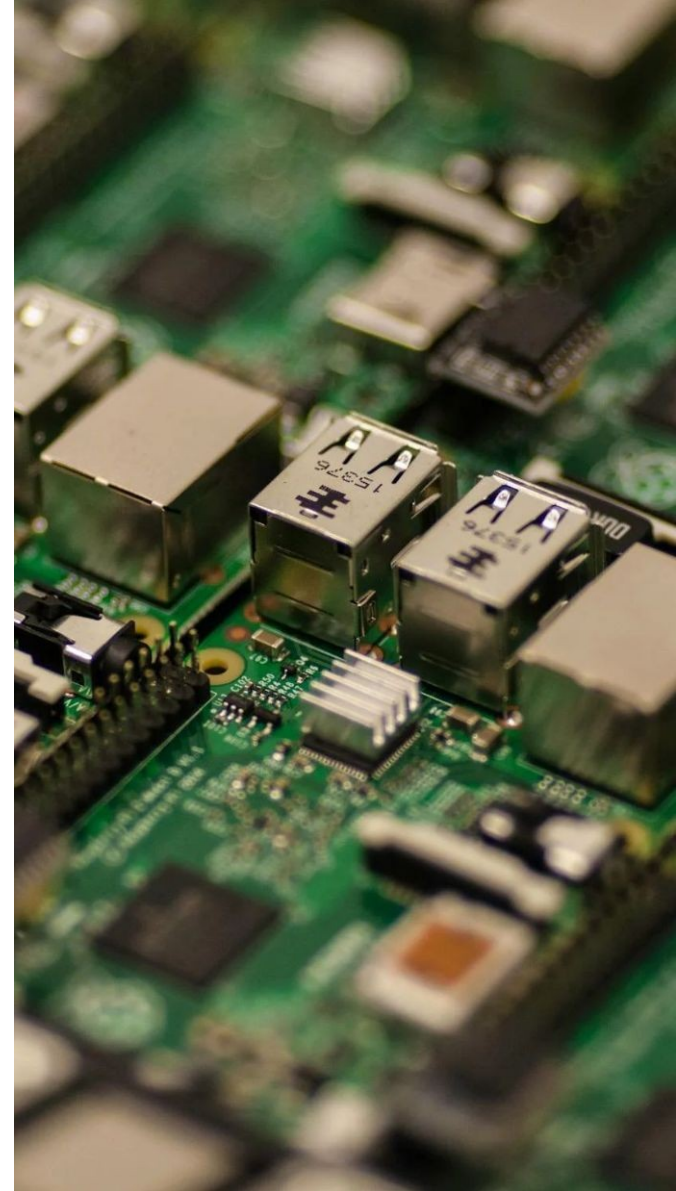
COPIA FORENSE E LETTURA DEL DATABASE

Copia forense

L'acquisizione forense può avvenire in modo classico, sia per i mini-PC di tipo x86 che per le Raspberry Pi.

Si ottiene **un'immagine disco** in formato DD o EWF, che può essere aperta con numerosi strumenti forensi.

Se l'installazione di Home Assistant è su una macchina virtuale, è sufficiente esportare il disco in un formato leggibile (tipicamente VMDK).





```
Welcome to the Home Assistant command line.
```

```
System information
IPv4 addresses for enp0s3: 192.168.1.10/24
IPv6 addresses for enp0s3: fe80::98f8:e057:f060:7007/64

OS Version:           Home Assistant OS 15.2
Home Assistant Core:  2025.5.3

Home Assistant URL:    http://homeassistant.local:8123
Observer URL:          http://homeassistant.local:4357
[core-ssh ~]$
```

Home Assistant OS

Il sistema operativo Hass.io è interamente basato su Docker.

Il partizionamento del disco è formato da otto volumi, che contengono essenzialmente programmi di sistema, file relativi al kernel o al funzionamento dei container.

L'unica partizione di nostro interesse è hassos-data.

Volume dati

FILE DI CONFIGURAZIONE

Relativi al *supervisor* della piattaforma

COMPONENTI AGGIUNTIVI

Eventualmente installati dall'utente

DATABASE STORICO

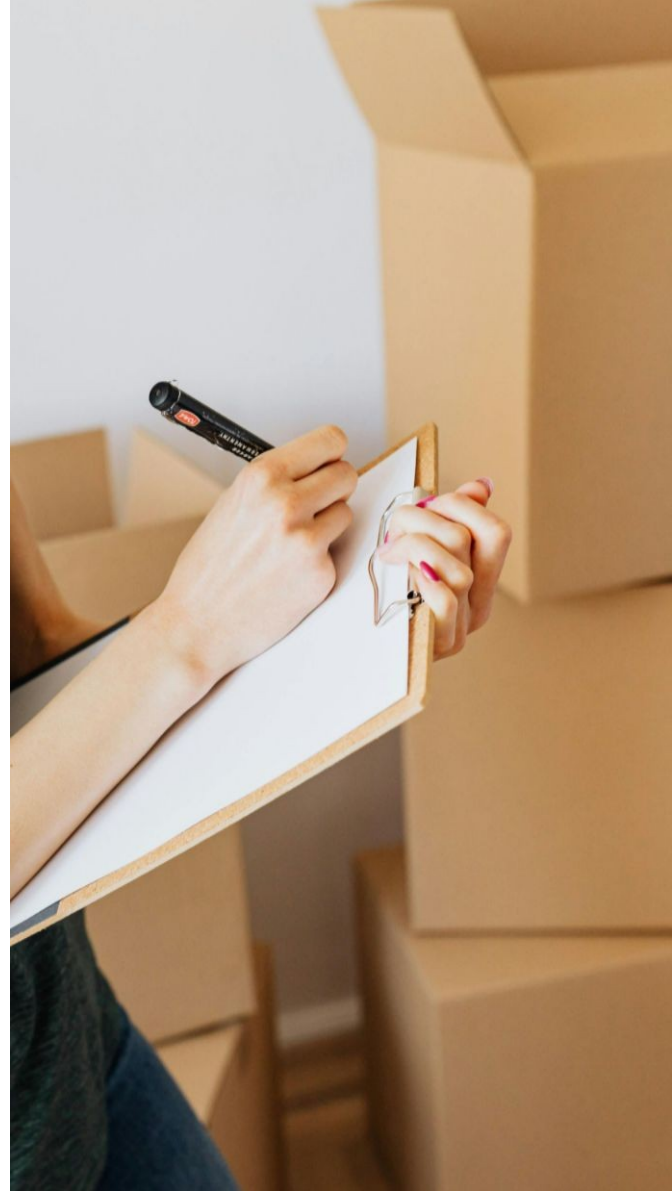
Con le registrazioni dei dati

File di configurazione

Le configurazioni del *supervisor* si trovano nella directory principale `/supervisor`, all'interno di alcuni file JSON.

Il file `addons.json` risulta di particolare interesse perché elenca i **componenti aggiuntivi ufficiali** che l'utente ha aggiunto alla propria installazione.

Le configurazioni applicative si trovano principalmente nel file `/supervisor/homeassistant/configuration.yaml` e alcuni altri file nella stessa directory.





Componenti aggiuntivi

I file di pertinenza dei componenti ufficiali si trovano in [/supervisor/addons](#) e [/supervisor/addon_config](#).

Inoltre, l'utente può aggiungere anche componenti "personalizzati" manualmente, oppure tramite la raccolta **HACS (*Home Assistant Community Store*)**.

Questi ultimi si trovano nella directory [custom_components](#) contenuta in [/supervisor/homeassistant](#).

Database storico

Il file **più importante** in assoluto è `home-assistant_v2.db`, contenuto in `/supervisor/homeassistant`.

Esso è un archivio SQLite che memorizza quanto occorso nel sistema: la cronologia degli eventi accaduti (*events*), i cambi di stato per le entità non numeriche (*states*) e quelli per le entità numeriche (*statistics*).

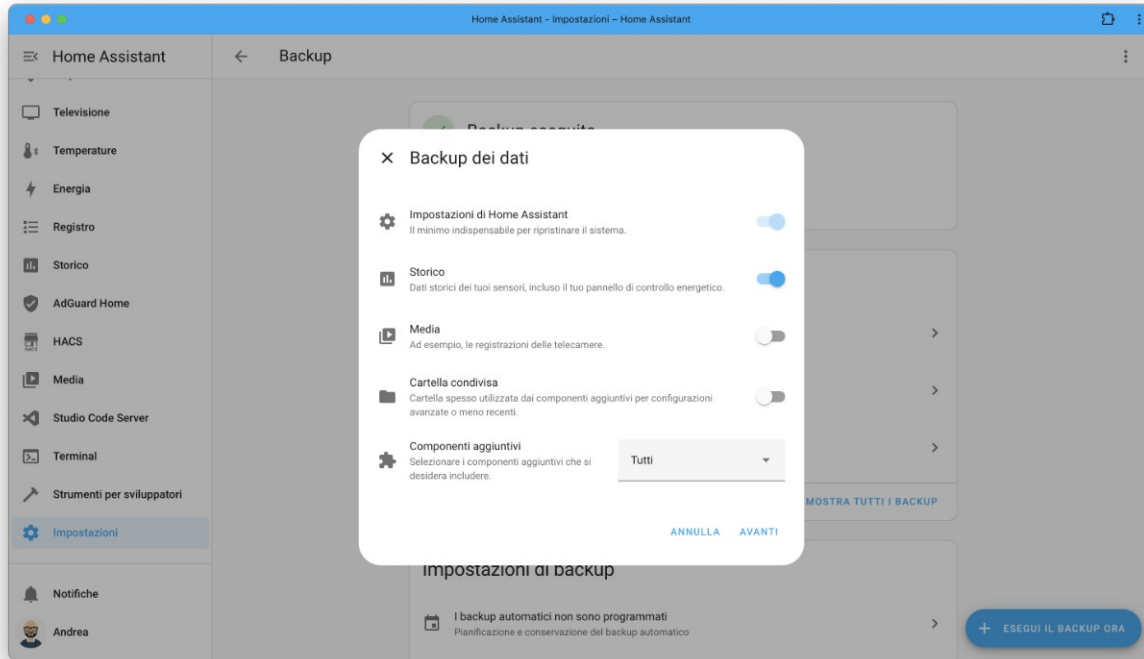
L'analisi del database storico con alcune query SQL ci permette di **estrarre moltissimi dati**.



ESPORTARE UN BACKUP

Se sono disponibili le credenziali del sistema, si può esportare un backup direttamente tramite l'interfaccia web.

Il backup di Home Assistant contiene il database integrale e tutti i componenti aggiuntivi.



Esempi pratici

QUALI RISPOSTE È POSSIBILE OTTENERE

AZIONAMENTO DEI DISPOSITIVI

Data di inizio - Data di fine

3 giu, 00:00 - 3 giu, 23:59

<

>

+ Scegli area

+ Scegli dispositivo

+ Scegli entità

+ Scegli l'etichetta



Spegnimento presa TV standby attivato dallo stato numerico di Televisione - power

14:41:19 - 5 giorni fa



Riscalda acqua per caffè spento attivato dall'automazione Attivazione De' Longhi attivato dallo stato di De' Longhi EC 201

14:39:18 - 5 giorni fa



Riscalda acqua per caffè acceso attivato dall'automazione Attivazione De' Longhi attivato dallo stato di De' Longhi EC 201

14:39:18 - 5 giorni fa



Riscalda acqua per caffè started attivato dall'automazione Attivazione De' Longhi attivato dallo stato di De' Longhi EC 201

14:39:18 - 5 giorni fa



Attivazione De' Longhi attivato dall'automazione Sensore De' Longhi ON attivato dallo stato di Potenza caffè

14:39:18 - 5 giorni fa



De' Longhi EC 201 acceso attivato dall'automazione Sensore De' Longhi ON attivato dallo stato di Potenza caffè

14:39:18 - 5 giorni fa



Sensore De' Longhi ON attivato dallo stato di Potenza caffè rilevato potenza

14:39:18 - 5 giorni fa



Potenza caffè rilevato potenza

14:39:18 - 5 giorni fa

RICERCA CON QUERY SQL

```
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
37	14199115	842E7C4B	052BF7F0	2025-06-03 14:39:18	automation.de_longhi_off	NULL	NULL	Sensore De' Longhi OFF	state of bi

Sensori ambientali

Grazie alle statistiche di Home Assistant, possiamo leggere i dati dei sensori eventualmente presenti nell'abitazione (dettagliatamente per i primi 10 giorni, poi ogni ora).

Esempi:

- Un calo improvviso di umidità in una determinata stanza può indicare l'apertura di una finestra
- Un picco di umidità in bagno indica l'uso della doccia
- Un consumo di Watt cospicuo può indicare l'uso di un elettrodomestico come la lavatrice

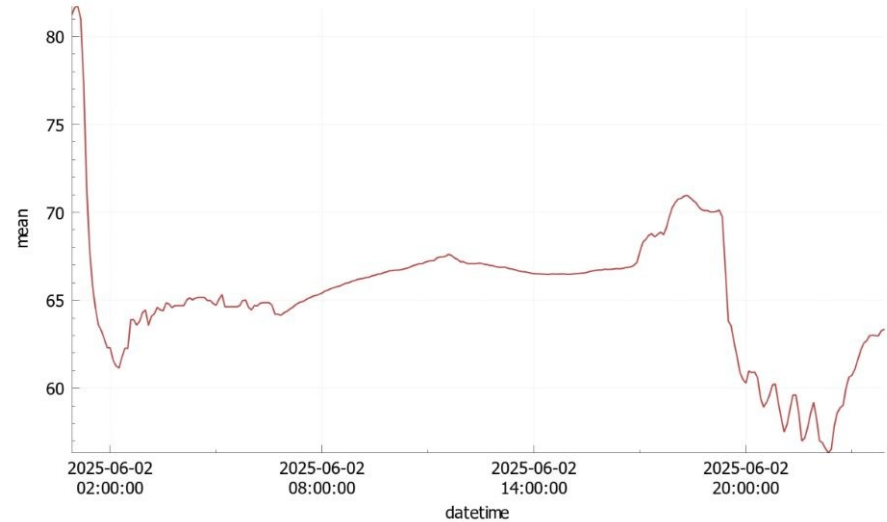


Generazione del grafico

Usando DB Browser for SQLite possiamo generare un grafico per questa 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
```

Il valore 38 per “umidità bagno” è stato ricavato dalla tabella `statistics_meta`.





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

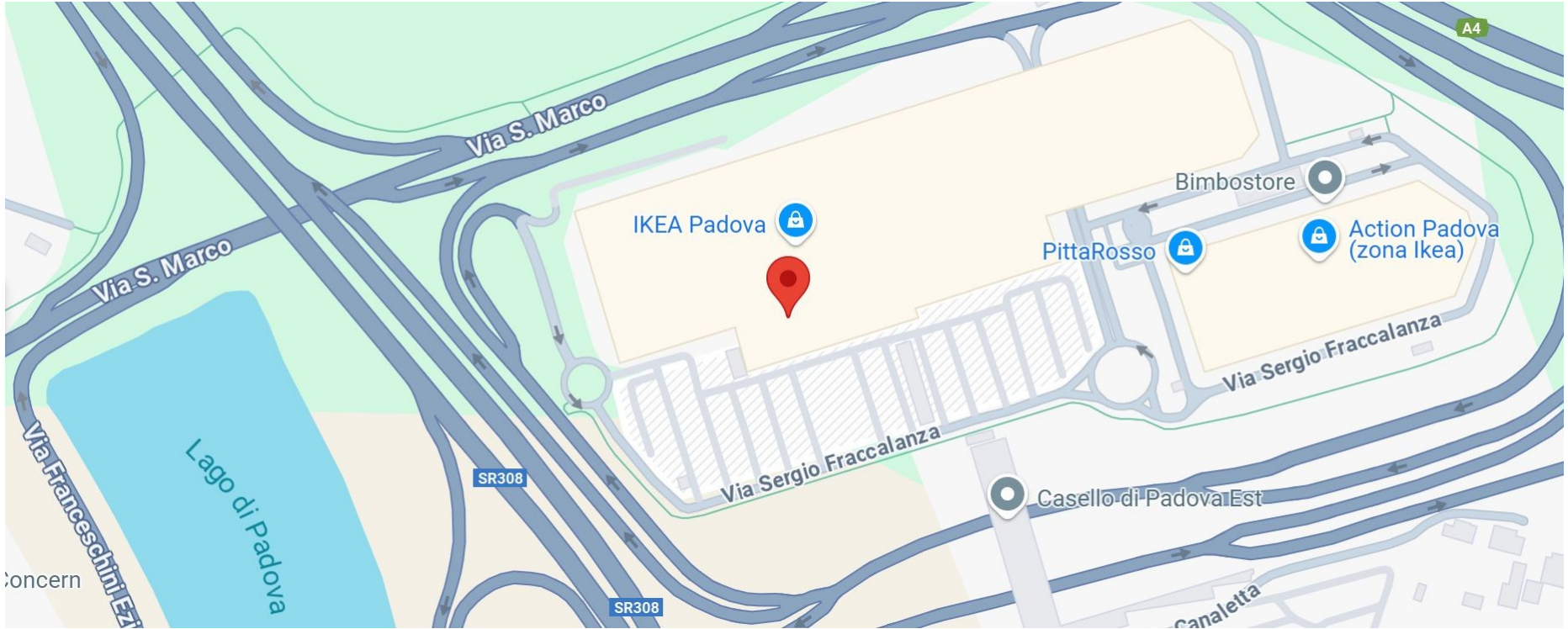
— JOHN MCAFEE

POSIZIONI REGISTRATE DALL'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

RISULTATO



CONTATTI

Web

andrealazzarotto.com

GitHub

[Lazza](#)

X / Twitter

[@thelazza](#)

Mastodon

[@lazza@mastodon.social](#)

