D4 Project

Open and collaborative network monitoring

Team CIRCL
https://www.d4-project.org/

20190307

Aurélien Thirion, Jean-Louis Huynen

Problem statement

- CSIRTs (or private organisations) build their **own honeypot, honeynet or blackhole monitoring network**
- Designing, managing and operating such infrastructure is a tedious and resource intensive task
- **Automatic sharing** between monitoring networks from different organisations is missing
- Sensors and processing are often seen as blackbox or difficult to audit

Objective

- Based on our experience with MISP[1] where sharing played an important role, we transpose the model in D4 project
- Keeping the protocol and code base **simple and minimal**
- Allowing every organisation to **control and audit their own sensor network**
- Extending D4 or **encapsulating legacy monitoring protocols** must be as simple as possible
- Ensuring that the sensor server has **no control on the sensor** (unidirectional streaming)
- Don't force users to use dedicated sensors and allow **flexibility of sensor support** (software, hardware, virtual)

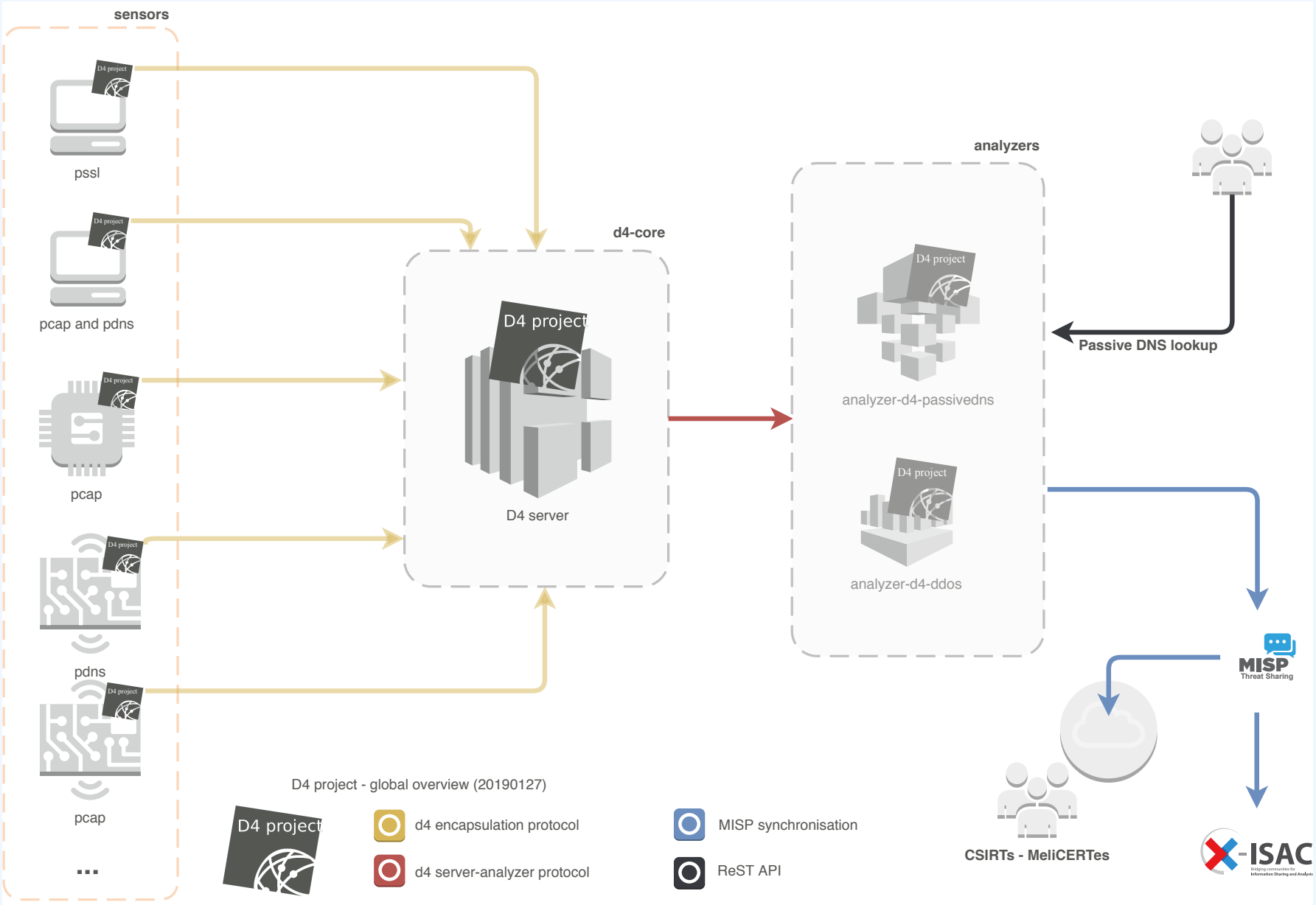
[1] https://github.com/MISP/MISP

(short) History

- D4 Project (co-funded under INEA CEF EU program) started - 1st November 2018
- D4 encapsulation protocol version 1 published - 1st December 2018
- v0.1 release of the D4 core[2] including a server and simple D4 C client - 21st January 2018
- First version of a golang D4 client[3] running on ARM, MIPS, PPC and x86 - January 2018

[2] https://www.github.com/D4-project/d4-core
[3] https://www.github.com/D4-project/d4-goclient/

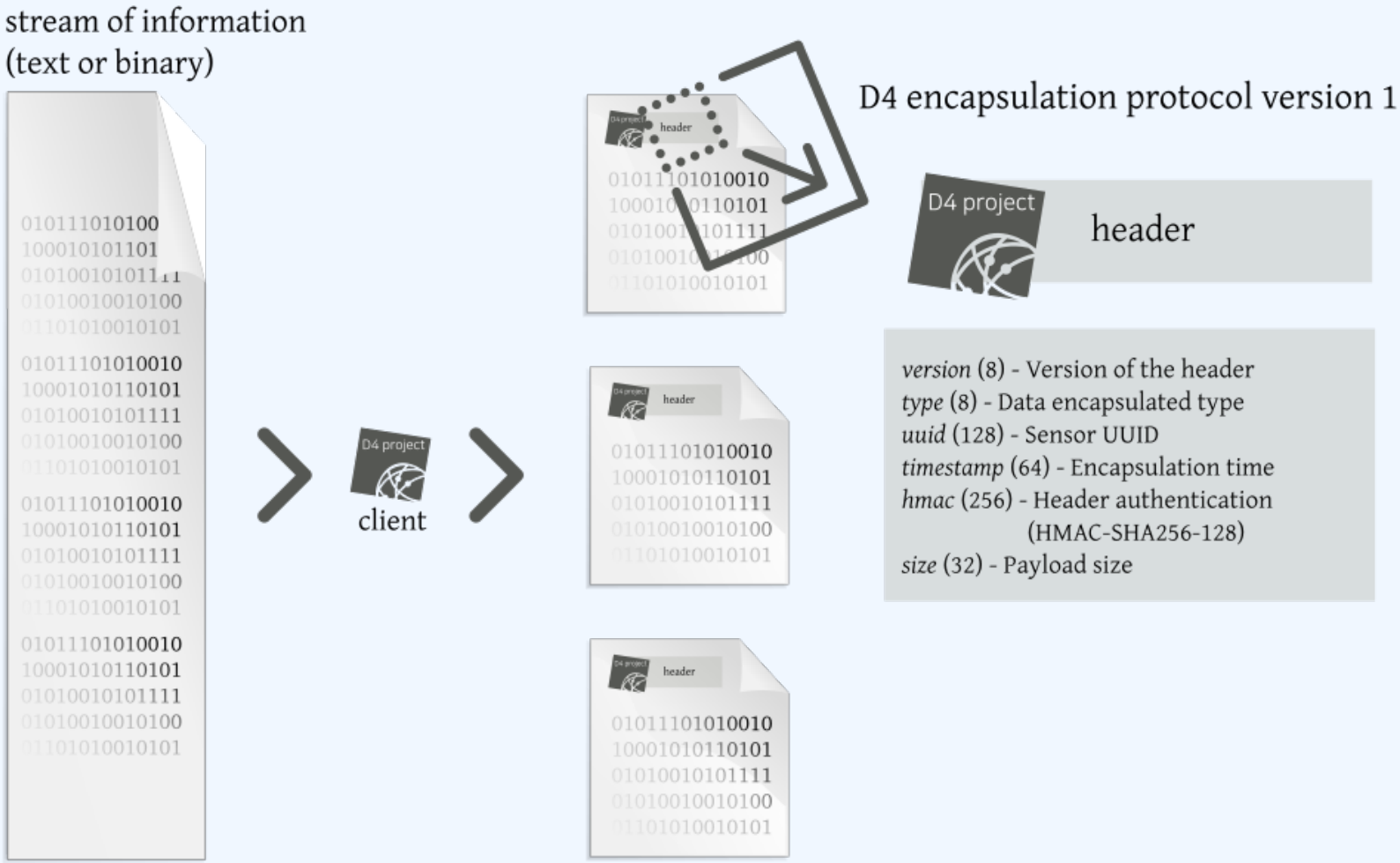
D4 Overview


sensors
pssl
pcap and pdns
pcap
pdns
pcap
...
d4-core
D4 project
D4 server
analyzers
analyzer-d4-passivedns
analyzer-d4-ddos
Passive DNS lookup
MISP
Threat Sharing
CSIRTs - MeliCERTes
-ISAC
D4 project - global overview (20190127)
D4 project
d4 encapsulation protocol
d4 server-analyzer protocol
MISP synchronisation
ReST API

Roadmap (next 2 months)

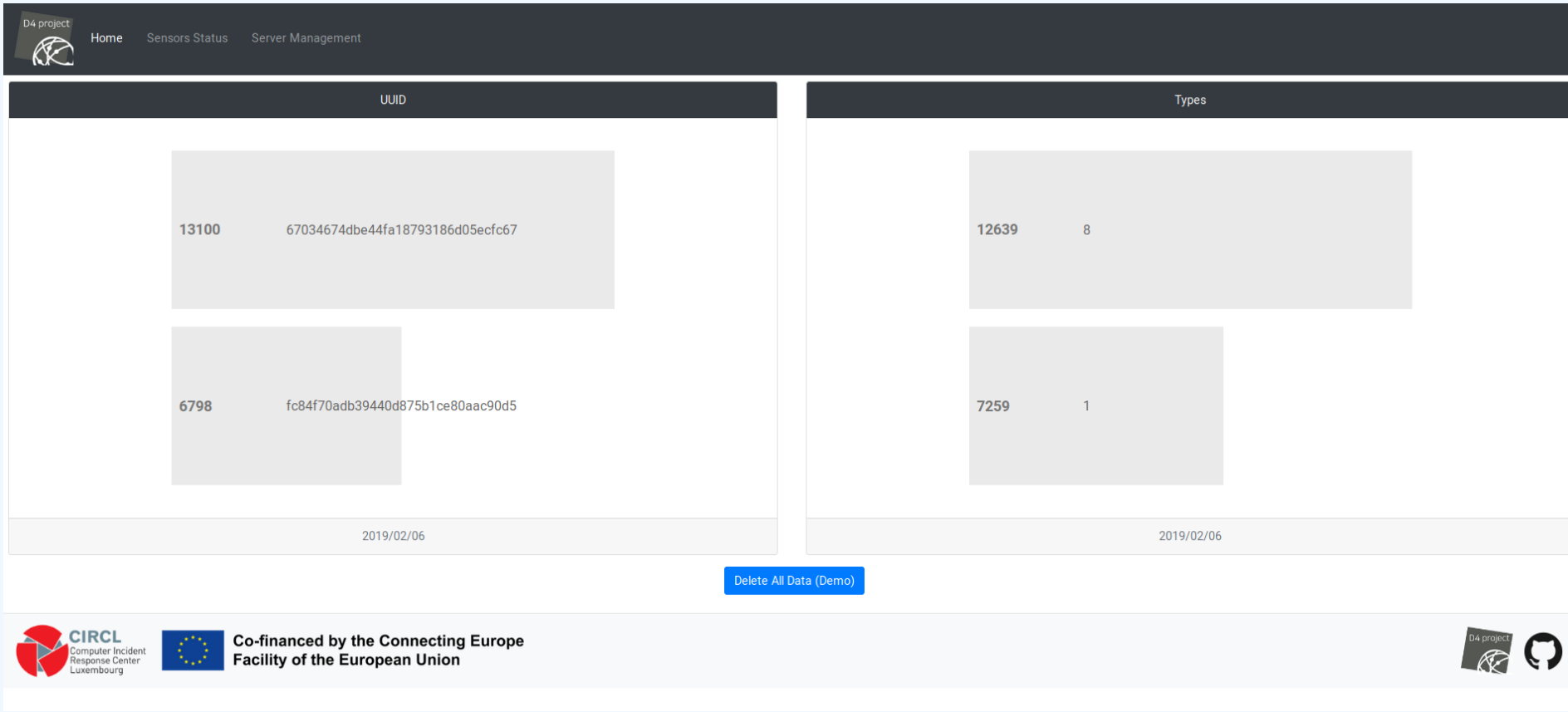
- Passive DNS analyzer (alpha version released)
- Passive SSL collector and analyzer
- Backscatter DDoS traffic analyzer
- **Default server** (blackhole monitoring or Passive DNS collector) at CIRCL for organisations willing to contribute without running their own D4 server

D4 encapsulation protocol

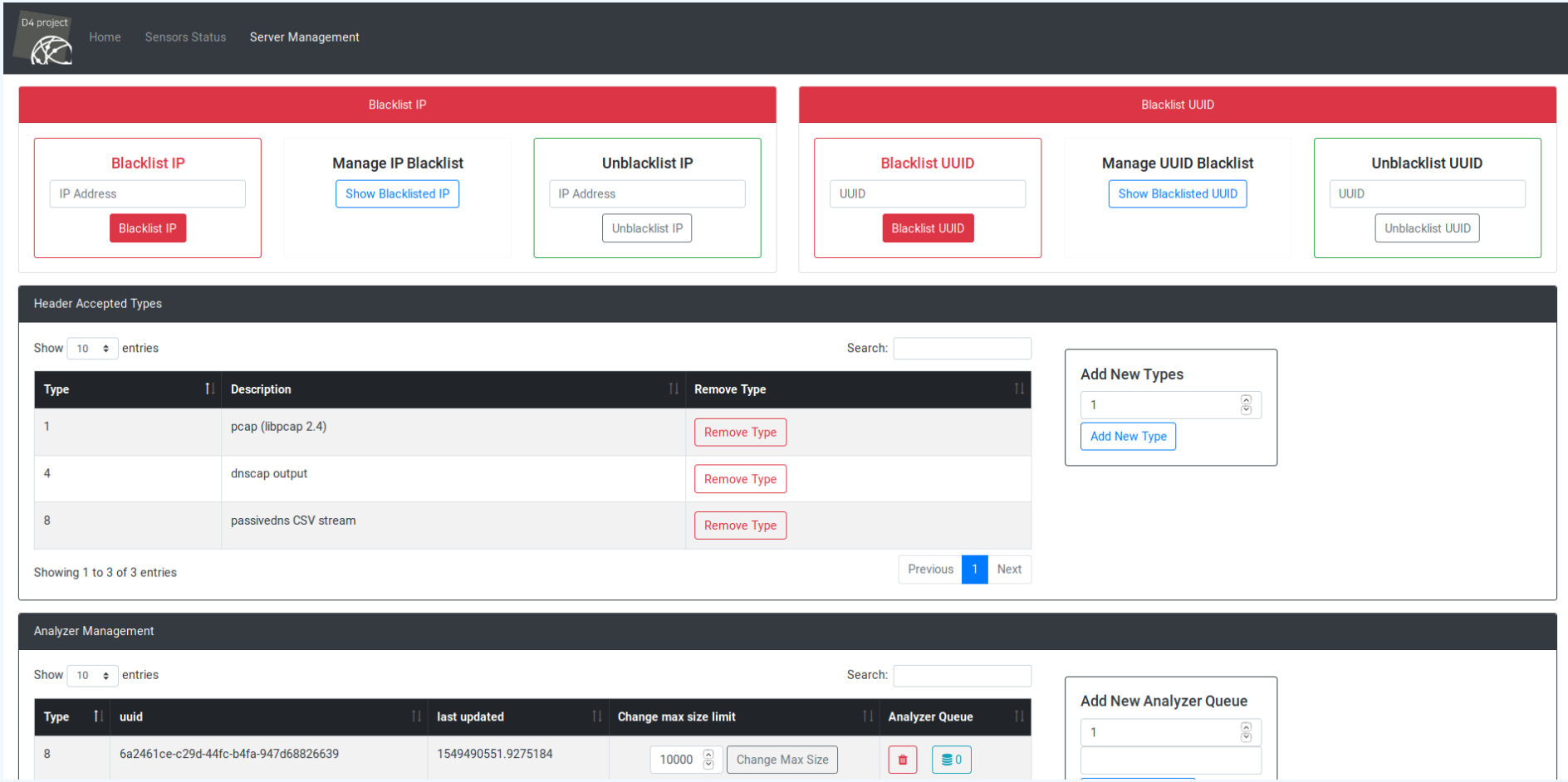


https://www.d4-project.org

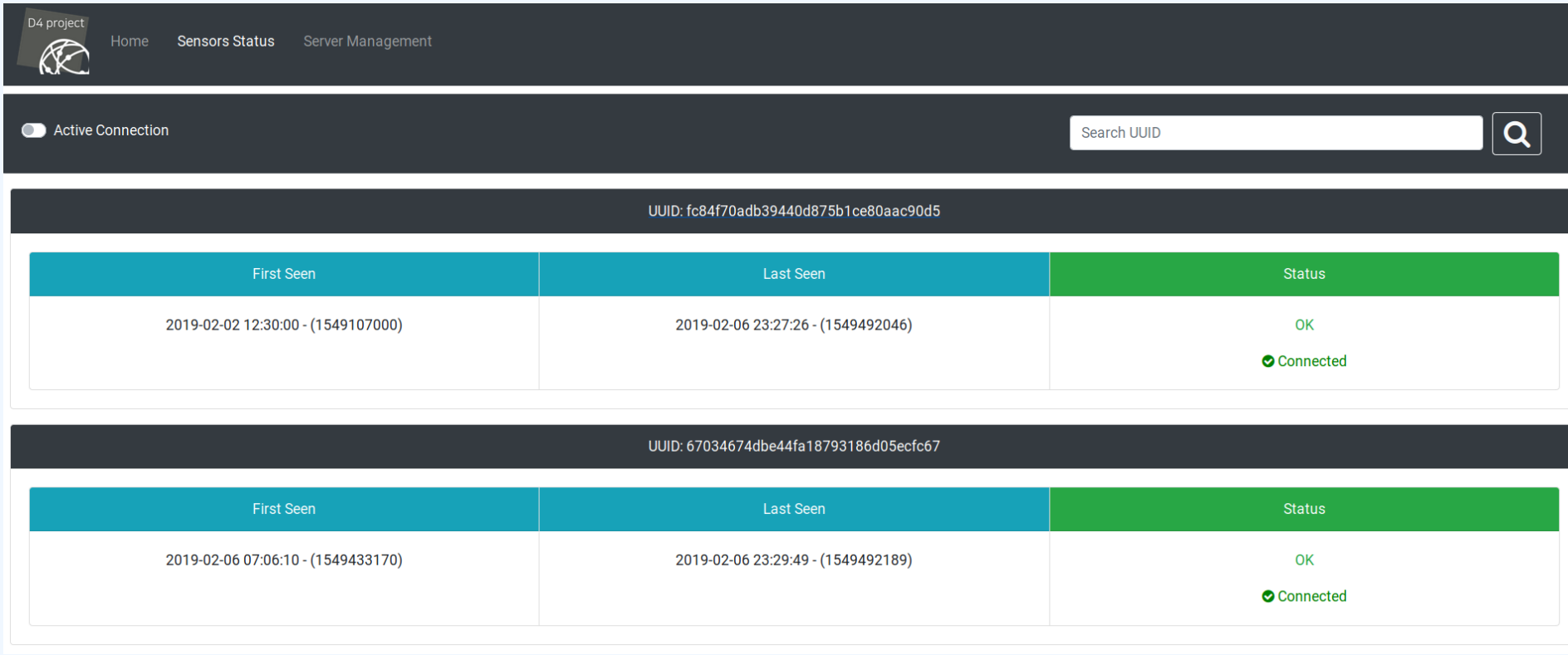
D4 SERVER - MAIN INTERFACE



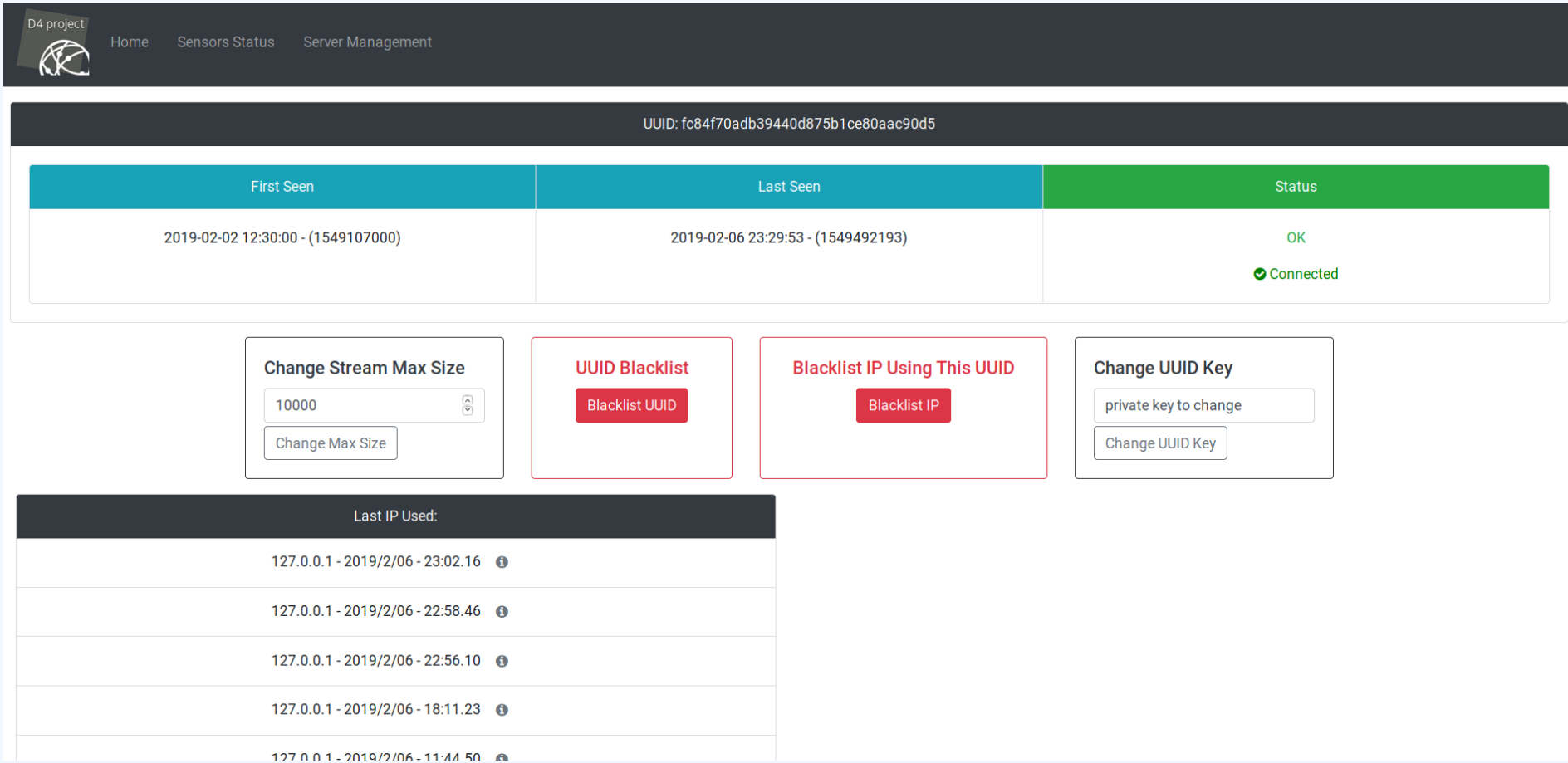
D4 server - server management



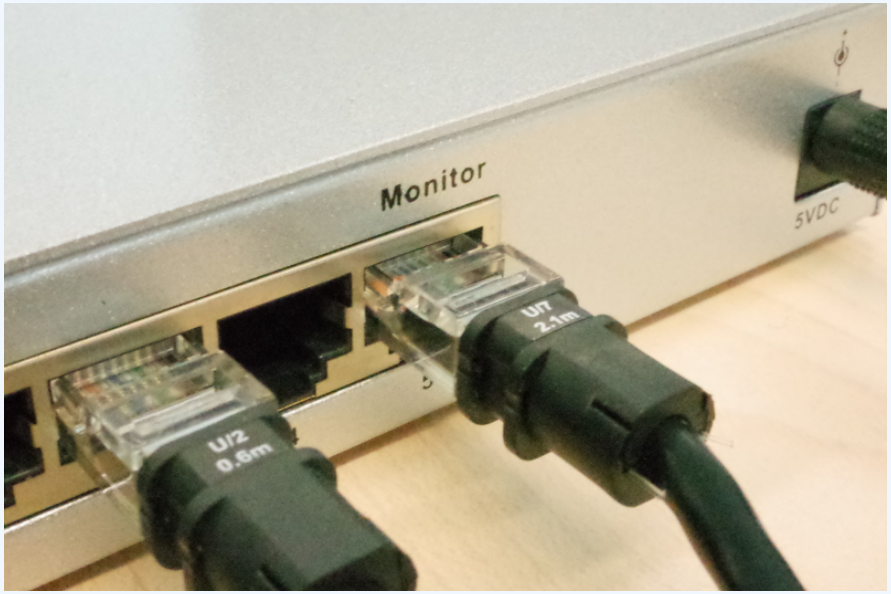
D4 server - sensor overview

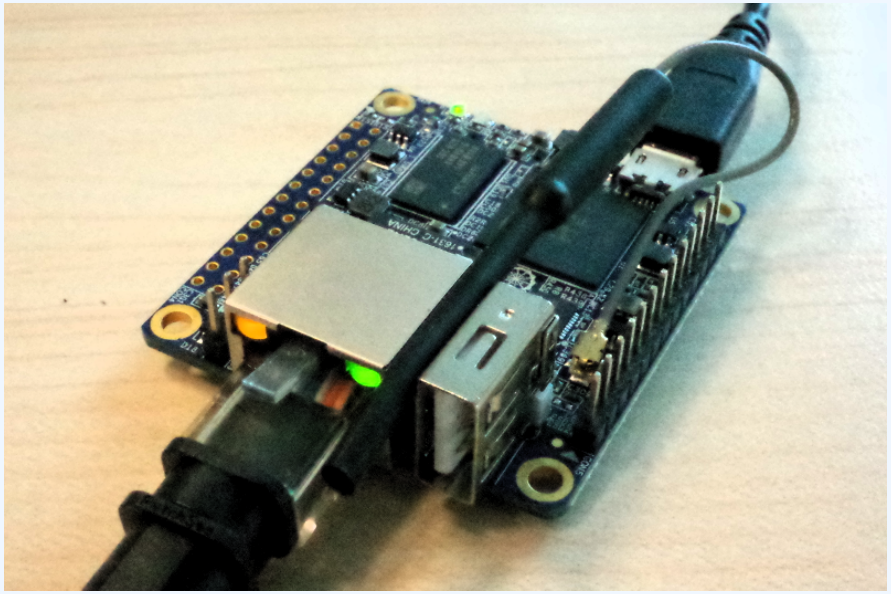


D4 server - sensor management



D4 client example : A passive SSL fingerprinter





- 1 desktop monitored during 15 days
- 3327 TLS sessions fingerprinted
- 600 unique certificates collected

Get in touch if you want to join the project, host a sensor or contribute

- Collaboration can include research partnership, sharing of collected streams or improving the software.
- Contact: info@circl.lu
- `https://github.com/D4-Project` - `https://twitter.com/d4_project`