D4 Project

Open and collaborative network monitoring

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

2019/05/21

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

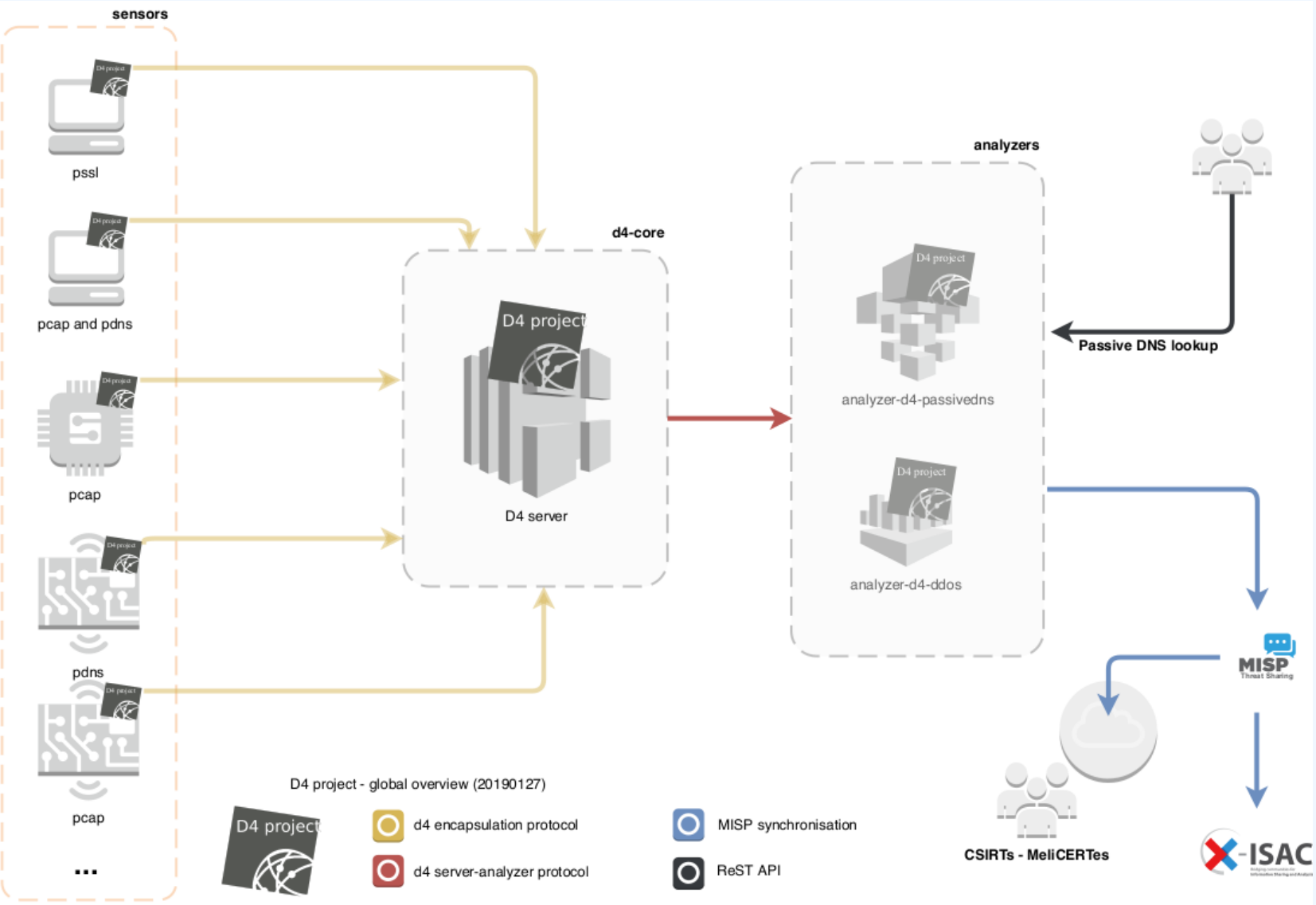
- D4 Project (co-funded under INEA CEF EU program) started - 1st November 2018
- D4 encapsulation protocol version 1 published - 1st December 2018
- v0.1 release of the D4 core[2] including a server and simple D4 C client - 21st January 2019
- First version of a golang D4 client[3] running on ARM, MIPS, PPC and x86 - 14th February 2019

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

(short) History

Release	Date
analyzer-d4-passivedns-v0.1	Apr. 5, 2019
analyzer-d4-passivessl-0.1	Apr. 25, 2019
analyzer-d4-pibs-v0.1	Apr. 8, 2019
BGP-Ranking-1.0	Apr. 25, 2019
d4-core-v0.1	Jan. 25, 2019
d4-core-v0.2	Feb. 14, 2019
d4-core-v0.3	Apr. 8, 2019
d4-goclient-v0.1	Feb. 14, 2019
d4-goclient-v0.2	Apr. 8, 2019
d4-server-packer-0.1	Apr. 25, 2019
IPASN-History-1.0	Apr. 25, 2019
sensor-d4-tls-fingerprinting-0.1	Apr. 25, 2019

D4 Overview

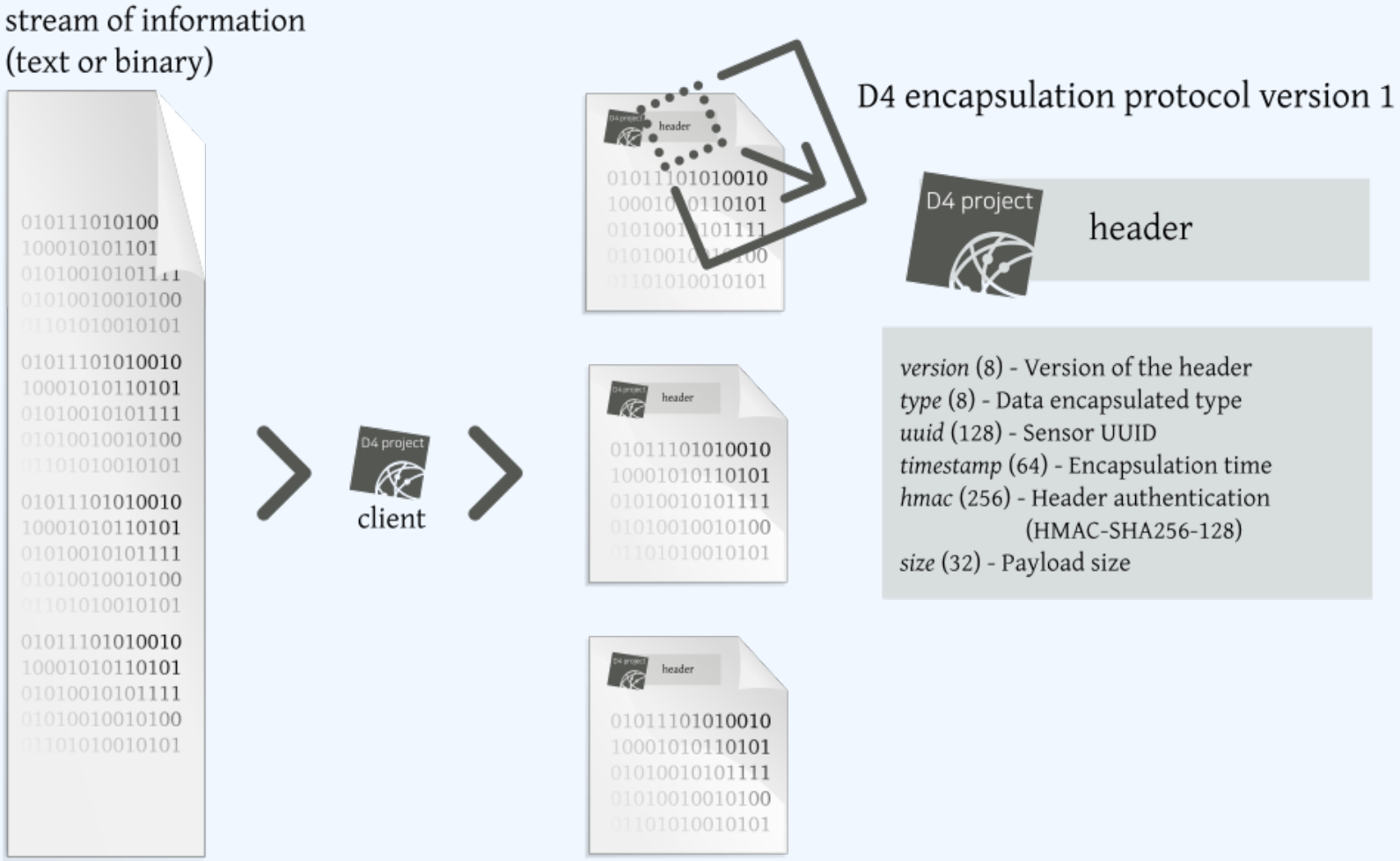

sensors
pssl
pcap and pdns
pcap
pdns
pcap
...
d4-core
D4 project
D4 server
analyzers
D4 project
analyzer-d4-passivedns
D4 project
analyzer-d4-ddos
Passive DNS lookup
MISP
Threat Sharing
CSIRTs - MeliCERTes
X-ISAC
D4 project - global overview (20190127)
D4 project
d4 encapsulation protocol
d4 server-analyzer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

Roadmap

- CIRCL will host an instance for organisations willing to contribute without running their own D4 server, as well as for free-riders:
  - Passive DNS collector / analyzer / lookup service
  - Passive SSL collector / analyzer / lookup service
- Closely followed by:
  - Backscatter DDoS traffic analyzer

D4 Overview

D4 encapsulation protocol



https://www.d4-project.org

D4 Header

Name	bit size	Description
version	uint 8	Version of the header
type	uint 8	Data encapsulated type
uuid	uint 128	Sensor UUID
timestamp	uint 64	Encapsulation time
hmac	uint 256	Authentication header (HMAC-SHA-256-128)
size	uint 32	Payload size

D4 Header

Type	Description
0	Reserved
1	pcap (libpcap 2.4)
2	meta header (JSON)
3	generic log line
4	dnscap output
5	pcapng (diagnostic)
6	generic NDJSON or JSON Lines
7	generic YAF (Yet Another Flowmeter)
8	passivedns CSV stream
254	type defined by meta header (type 2)

D4 meta header

D4 header includes an easy way to **extend the protocol** (via type 2) without altering the format. Within a D4 session, the initial D4 packet(s) type 2 defines the custom headers and then the following packets with type 254 is the custom data encapsulated.

```
{
  "type": "ja3-jl",
  "encoding": "utf-8",
  "tags": [
    "tlp:white"
  ],
  "misp:org": "5b642239-4db4-4580-adf4-4ebd950d210f"
}
```

D4 server

- D4 core server[4] is a complete server to handle clients (sensors) including the decapsulation of the D4 protocol, control of sensor registrations, management of decoding protocols and dispatching to adequate decoders/analysers.
- D4 server is written in Python 3.6 and runs on standard GNU/Linux distribution.

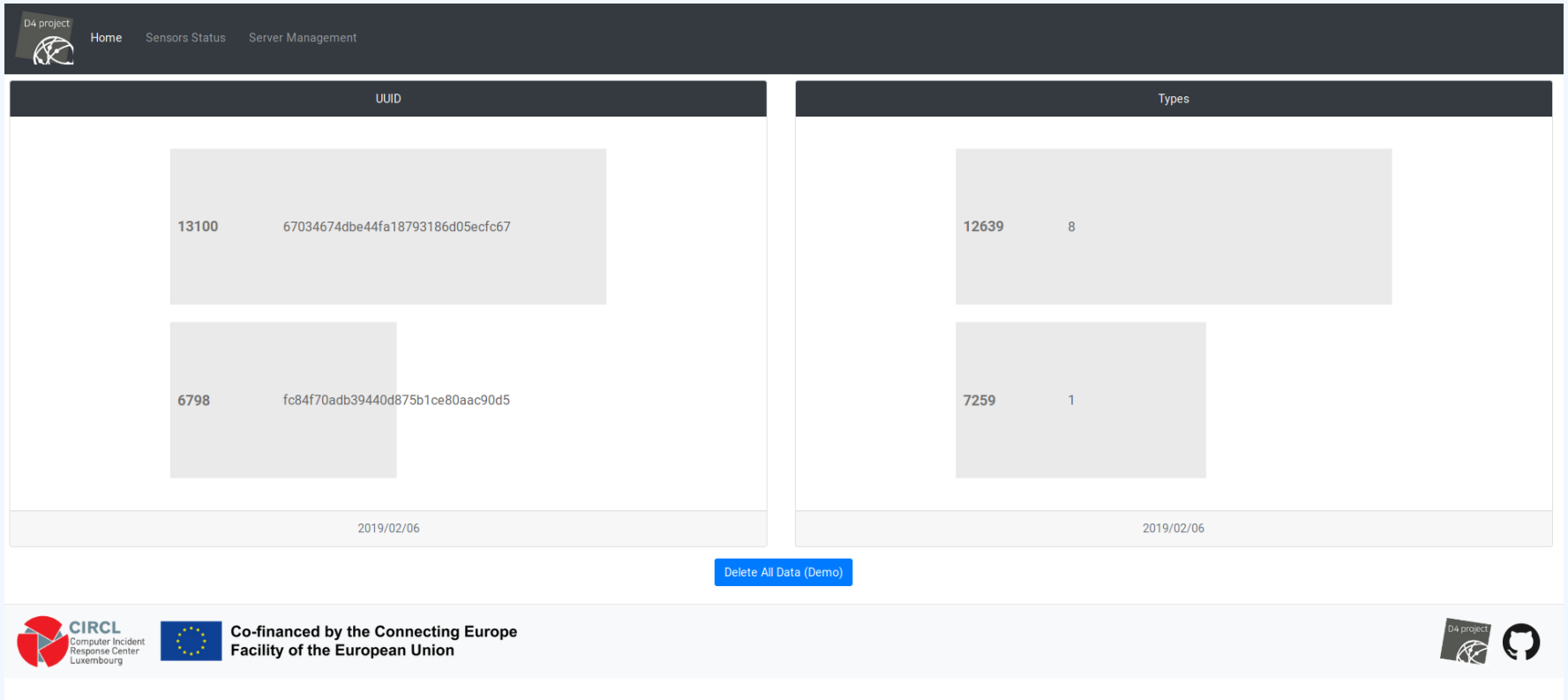
[4] https://github.com/D4-project/d4-core

D4 server - management interface

The D4 server provides a web interface to manage D4 sensors, sessions and analyzer.

- Get Sensors status, errors and statistics
- Get all connected sensors
- Manage Sensors (stream size limit, secret key, ...)
- Manage Accepted types
- UUID/IP blocklist
- Create Analyzer Queues

D4 SERVER - MAIN INTERFACE



D4 SERVER - SERVER MANAGEMENT

D4 project

Home Sensors Status Server Management

Blacklist IP

Blacklist IP
IP Address
Blacklist IP

Manage IP Blacklist
Show Blacklisted IP

Unblacklist IP
IP Address
Unblacklist IP

Blacklist UUID

Blacklist UUID
UUID
Blacklist UUID

Manage UUID Blacklist
Show Blacklisted UUID

Unblacklist UUID
UUID
Unblacklist UUID

Header Accepted Types

Show 10 entries Search:

Type	Description	Remove Type
1	pcap (libpcap 2.4)	Remove Type
2	meta header (JSON)	Remove Type
4	dnscap output	Remove Type
8	passivedns CSV stream	Remove Type
254	type defined by meta header (type2)	Remove Type

Showing 1 to 5 of 5 entries Previous 1 Next

Show 10 entries Search:

Add New Types
1
Add New Type

D4 SERVER - SERVER MANAGEMENT

Show 10 entries Search:

Type Name	Description	Remove Type
ja3-jl		Remove Extended Type

Showing 1 to 1 of 1 entries Previous 1 Next

Analyzer Management

Show 10 entries Search:

Type	uuid	last updated	Change max size limit	Analyzer Queue
1	404d4594-7881-4643-85bf-b11f7d9436e8	1553608013.429933	10000 Change Max Size	3
4	ccb9548c380f4dd19ad3b1e94412e79a	Never	10000 Change Max Size	0

Showing 1 to 2 of 2 entries Previous 1 Next

Show 10 entries Search:

Type Name	uuid	last updated	Change max size limit	Analyzer Queue
ja3-jl	ccb9548c380f4dd19ad3b1e94412e79a	Never	10000 Change Max Size	0

Showing 1 to 1 of 1 entries Previous 1 Next

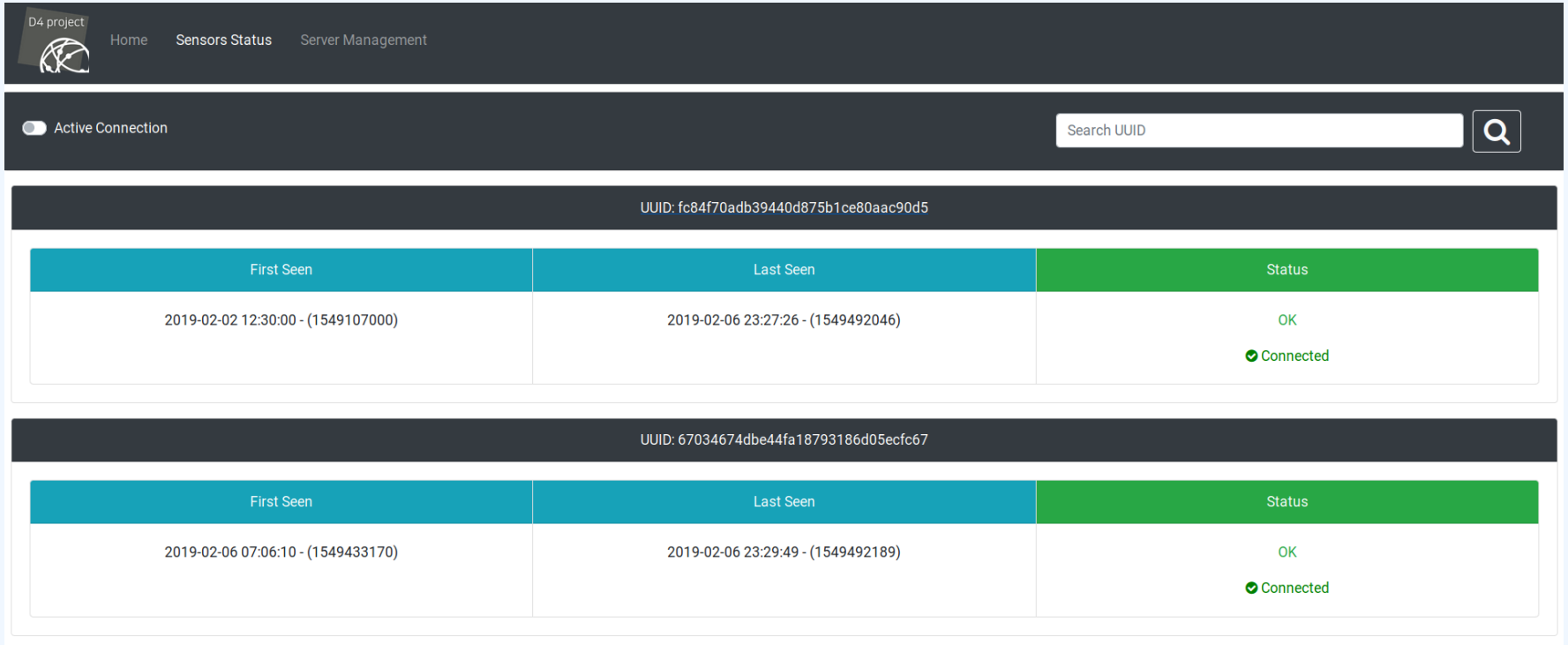
Add New Analyzer Queue

1

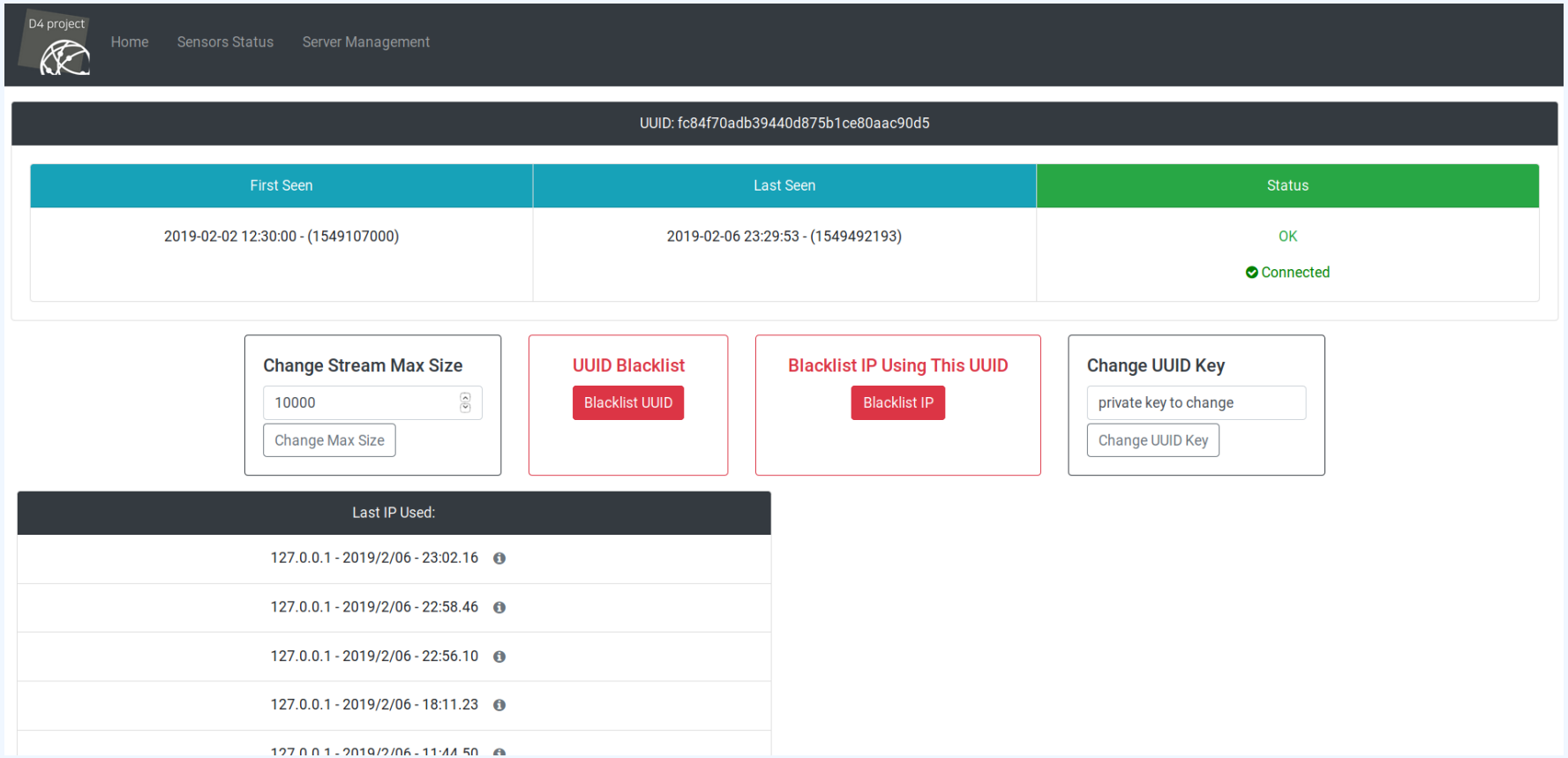
Analyzer uuid

Add New Analyzer

D4 SERVER - SENSOR OVERVIEW



D4 SERVER - SENSOR MANAGEMENT



Passive DNS

Passive SSL

Passive Identification of BackScatter traffic

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`