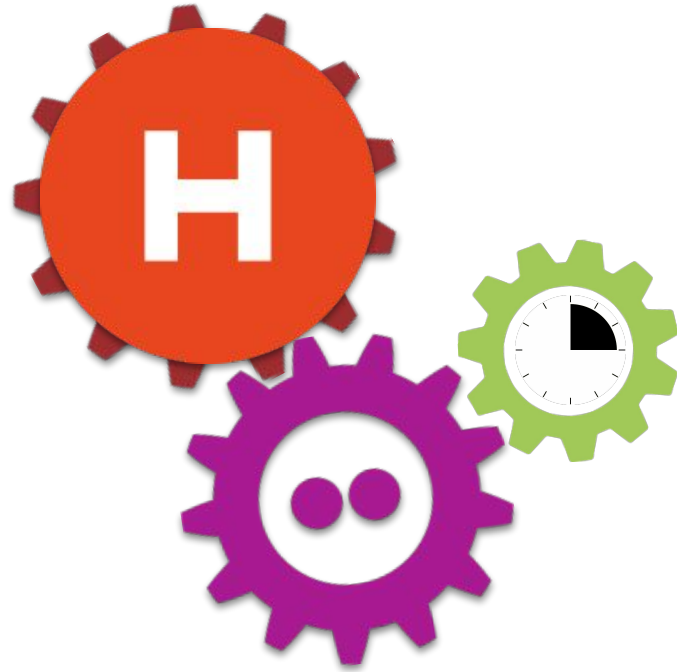




**WE ARE
MISSION
OSS FAMILY**

QXIP BV, AMSTERDAM **CAPTURE YOUR RTC HEARTS WITH HOMER**

ALEXANDR DUBOVIKOV (CTO, FOUNDER), LORENZO MANGANI (CEO),
CELESTE (CFO), DARIO (TPM), FEDERICO CABIDDU, GIACOMO VACCA,
EUGEN BIEGLER, MICHELE CAMPUS, GAETANO GARGIULO,
OPENSIPS TEAM, KAMAILIO TEAM, ASTERISK TEAM, FREESWITCH,
JANUS MEETECH, MEDIASOUP AMIGOS & ALL OUR FRIENDS

still
HOMER IS ALIVE!



*The next **HOMER** has been long overdue!*

*We aimed **really, really, really high** in terms of features and design requirements*

*We're a very small group, struggling to maintain **old** and **create new versions***

We are self-sponsored FOSS (more on this later)

what is...
HOMER



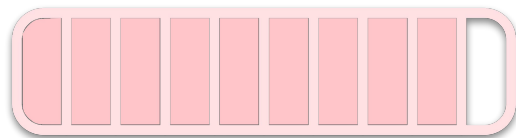
A Centralized Packet Capture System to Index and Troubleshoot **VoIP** and **RTC** Traffic

Natively supported by awesome projects such as **OpenSIPS, Kamailio, Asterisk, Freeswitch, Janus**
Alive and Kicking since 2011 (applause for surviving if you know how hard it gets for small fish)

what is...

HOMER SEVEN?

SIX WAS A DEVELOPMENT VERSION



HOMER 6.90%

*"We are products of our
past, but we don't have to
be prisoners of it."*

PAST → FUTURE

HOMER 5.x

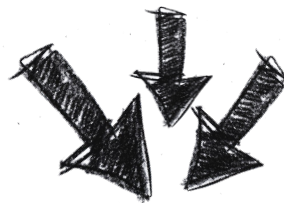
- ~~Stale Project & Codebase~~
- ~~Complex Installation Steps~~
- ~~Monolithic Configuration~~
- ~~Agents too complex to configure~~
- ~~Steep entrypoint for Developers~~
- ~~Too Few Protocols~~
- ~~Too Basic Statistics~~
- ~~Static Correlation~~
- ~~Minimal RTC Features~~
- ~~Outdated User Interface~~

HOMER 7.x

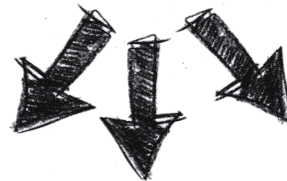
- Clean, Extended Project Ecosystem
- **Simplified Installation** & Less Moving Parts
- Switch to **Modular Configuration**
- **More Agents**, More Options for Everyone
- Clean, Standardized, Documented Code
- **Protocol Agnostic** at the Core/DBs
- Customizable **Metrics Exporters**
- **Distributed Correlation** using Graph DBs
- **RTC Ready** (*statistics + protocol events*)
- *Redesigned User-Interface (in development)*

COOL STORY BRO.

WHAT IS THE AGENDA



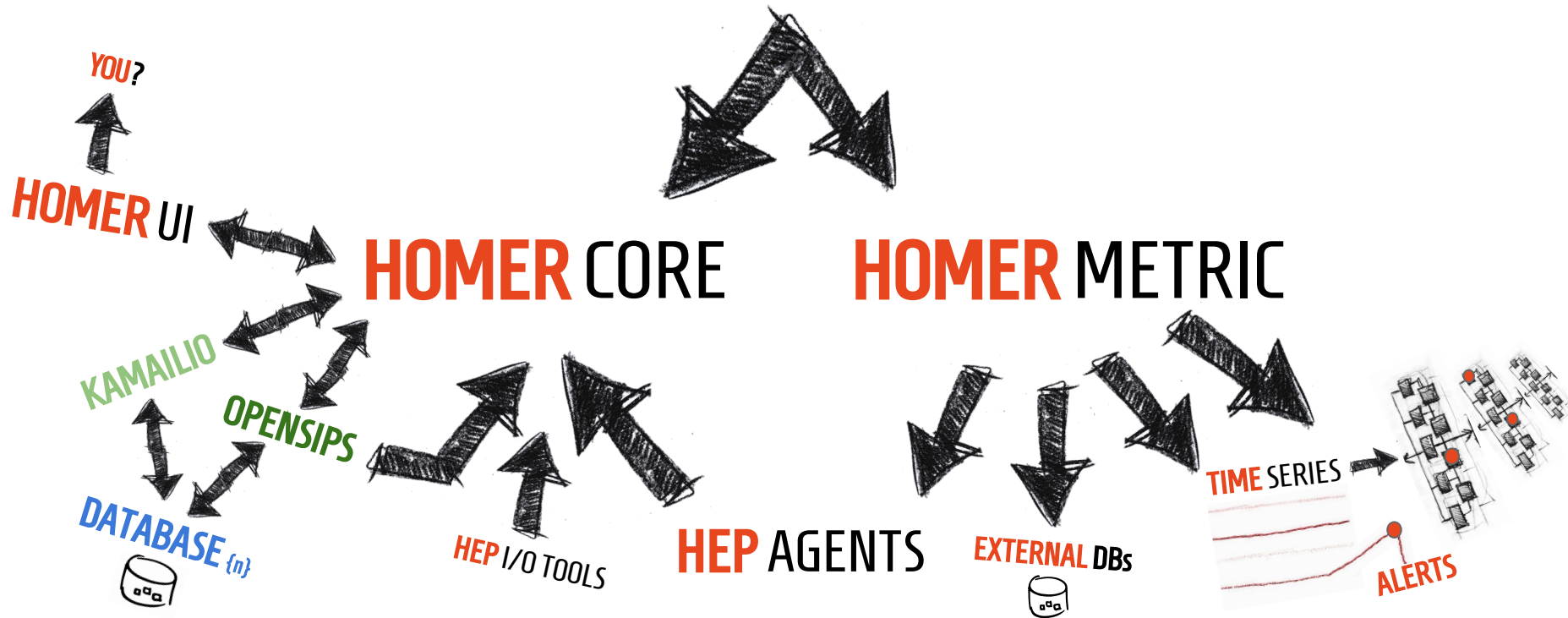
let's **CAPTURE** **EVERYTHING**
then **CORRELATE**
and **EXPORT** **EVERYWHERE** *possible



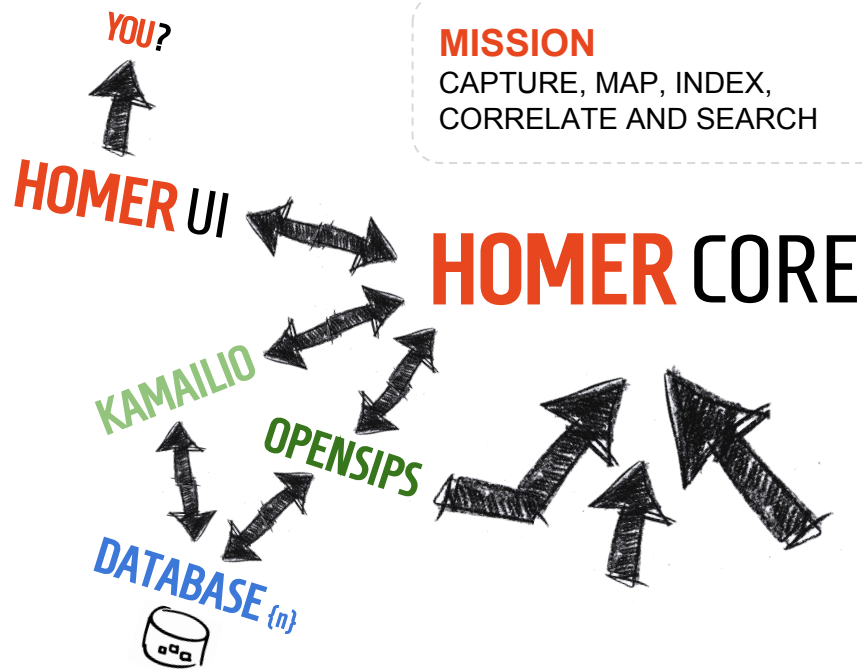
AMBITIOUS.

THE FULL PICTURE

HOMER SEVEN



HOMER SEVEN



MISSION

CAPTURE, MAP, INDEX,
CORRELATE AND SEARCH

HOMER CORE is the new fulcrum of the Project

NEW API:

Developed in Node JS from the ground up, following the best standards for stability and extensibility. *Bye PHP!*

NEW DB SCHEMA:

Fully leveraging the latest JSON datatype features in MySQL 5.7 and 8+ to provide a powerful and flexible storage to the HOMER and HEP ecosystem

NEW HEP TYPES:

OpenSIPS 2.3+ and Kamailio 5+ both provide great features enhancing and extending the monitoring and capture capabilities of HOMER

HOMER SEVEN

HOMER METRIC is the Statistics Shop of the stack

SMART:

We're not reinventing the wheel - there are many projects out there providing great Time Series monitoring and Alerting, and the smart choice is always to integrate.

FLEXIBLE:

There's no one stop shop for anything nowadays. HOMER allows you to use multiple export backends in parallel.

EXTENSIBLE:

Every available feature and module are an opportunity. Fancy something custom? Pipe everything to paStash and define your own logic using Node JS and NPM modules.

MISSION

EXPORT AND FORK METRICS TO MULTIPLE EXTERNAL TARGETS

HOMER METRIC



HOMER SEVEN

INGRESS HEP AGENTS

Your classic HEP Agents, enhanced with the latest features and protocol Types

CaptAgent

- SIP, TLS, RTCP, Diameter

HEPlify

- SIP, RTCP, DNS

HoracliFix - HepFix

- Oracle SIP, RTCP, RTC

OpenSIPS

- SIP, REST, MI, LOGS

paStash

- CDRs, File, Websocket, Net
- Janus RTC Events
- MediaSoup Events
- Freeswitch ESL
- Asterisk AMI

.. and more!

MISSION

IMPORT, EXPORT AND
FORK HEP STACK DATA



EGRESS HEP AGENTS

Agents interfacing with the rest of the data world, allowing parallel export and manipulation of data and statistics

PaStash

- Elasticsearch
- Splunk
- Statsd
- Redis
- Kafka
- GunDB
- ZeroMQ
- MQTT
- AMQP
- NSQ
- HEP
- HTTP/S

... and more!

HOMER CORE

The **key** feature of our next-generation platforms will be the ability to grow the supported stack quickly and being able to define and add **new protocols** and **event types** expressed and transported by a generic or dedicated **HEP subtypes**.

The design allows automatically mapping received protocols to schemas using self-determined matching or user defined configuration for granular control over data indexing strategy and cross-correlation for extracted protocol field elements.

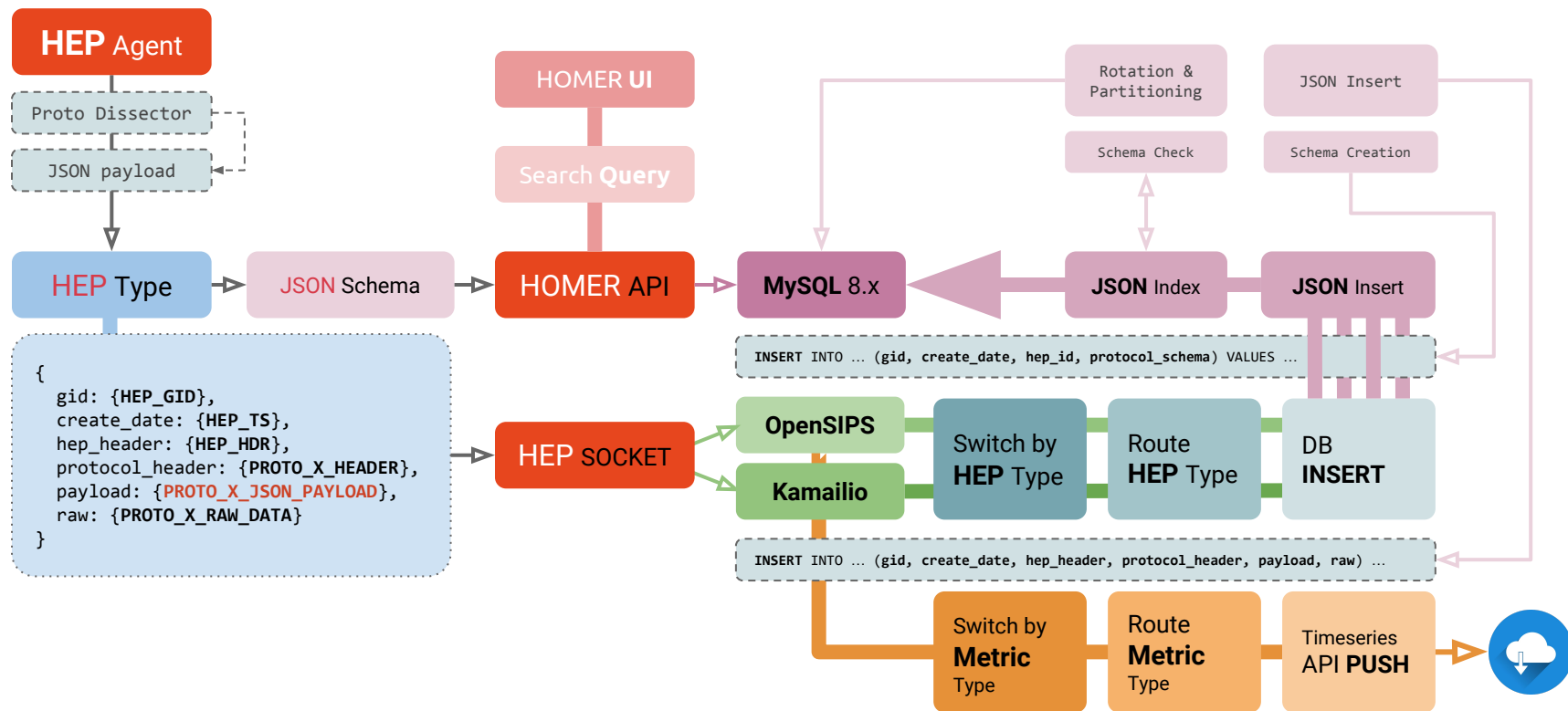
All new protocols will be first-class citizen and feature full search, visualization and correlation features the stack offers.

The new HEP sources include HEPlify, OpenSIPS 2.3+ (SIP, REST, MI, LOGS) Janus Gateway, Mediasoup and others!

SOUNDS COMPLEX?

A LOOK UNDER THE HOOD

HEP JSON



HEP JSON

HEP JSON : DNS Packet

```
#
U 127.0.0.1:48304 -> 127.0.0.1:9060
  HEP3.(.....)1.....5.....Zu.....5.....myhep.....{"id":59287,"qr":false,"opcode":0,"aa":false,"tc":false,"rd":
  true,"ra":false,"z":0,"rescode":0,"qdc":1,"anc":0,"nsc":0,"arc":0,"questions":[{"name":"www.fosdem.org","type":1,"class":1}]}
#
U 127.0.0.1:48304 -> 127.0.0.1:9060
  HEP3.'.....)1.....5.....Zu.%.....{.....5.....myhep.....{"id":6702,"qr":false,"opcode":0,"aa":false,"tc":false,"rd":t
  rue,"ra":false,"z":0,"rescode":0,"qdc":1,"anc":0,"nsc":0,"arc":0,"questions":[{"name":"www.fosdem.org","type":1,"class":1}]}
#
U 127.0.0.1:48304 -> 127.0.0.1:9060
  HEP3.(.....)1.....5.....Zu.0.....5.....myhep.....{"id":65452,"qr":false,"opcode":0,"aa":false,"tc":false,"rd":
  true,"ra":false,"z":0,"rescode":0,"qdc":1,"anc":0,"nsc":0,"arc":0,"questions":[{"name":"www.google.com","type":1,"class":1}]}
```



HEP JSON

HEP JSON DNS : Table Structure

```
mysql> show create table hep_proto_53_all_20171202\G
***** 1. row *****
Table: hep_proto_53_all_20171202
Create Table: CREATE TABLE `hep_proto_53_all_20171202` (
  `id` bigint(20) unsigned NOT NULL AUTO_INCREMENT,
  `gid` smallint(5) unsigned NOT NULL DEFAULT '0',
  `create_date` timestamp NOT NULL DEFAULT '1970-01-01 00:00:01',
  `hep_header` json NOT NULL,
  `protocol_header` json NOT NULL,
  `payload` json NOT NULL,
  `raw` varchar(2000) NOT NULL,
  PRIMARY KEY (`id`,`create_date`),
  KEY `create_date` (`create_date`)
) ENGINE=InnoDB AUTO_INCREMENT=90 DEFAULT CHARSET=utf8 ROW_FORMAT=COMPRESSED
```



HEP JSON

JSON DNS : Select Data

```
mysql> select * from hep_proto_53_all_20180203 WHERE JSON_EXTRACT(payload, "$.questions[0].name") = "google.com" \G
***** 1. row *****
  id: 89
  gid: 10
  create_date: 2017-12-02 15:13:06
  hep_header: {"proto": 53, "version": "3", "protocol": "hep", "time_sec": "1512227586", "time_usec": "151992", "timestamp": 1512227586, "capture_id": 102, "capture_ip": "127.0.0.1", "payload_len": 292, "correlation_id": ""}
  protocol_header: {"type": "ip", "vlan": 0, "ip_proto": 17, "protocol": "hep", "ip_family": 3, "source_ip": "172.93.49.177", "source_port": 42557, "destination_ip": "8.8.8.8", "destination_port": 53}
  payload: {"z": 0, "aa": false, "id": 65082, "qr": false, "ra": false, "rd": true, "tc": false, "anc": 0, "arc": 0, "nsc": 0, "qdc": 1, "opcode": 0, "rescode": 0, "questions": [{"name": "google.com", "type": 1, "class": 1}]}
  raw: {"data": [{"id": 65082, "qr": false, "opcode": 0, "aa": false, "tc": false, "rd": true, "ra": false, "z": 0, "rescode": 0, "qdc": 1, "anc": 0, "nsc": 0, "arc": 0, "questions": [{"name": "google.com", "type": 1, "class": 1}], "protocol": "json-dns", "timestamp": 1512227586, "hep_protocol": 53}
```

HEP JSON

JSON DNS : Select Data - Virtual Field/Keys

```
mysql> alter table hep_proto_53_all_20180203 add `host_name` varchar(255) GENERATED ALWAYS AS
(json_unquote(json_extract(`payload`, '$.questions[0].name'))) VIRTUAL NOT NULL;
```

```
mysql> select * from hep_proto_53_all_20180203 WHERE host_name = "google.com" \G
```

```
***** 1. row *****
```

id: 89

gid: 10

create_date: 2017-12-02 15:13:06

hep_header: {"proto": 0, "version": "3", "protocol": "hep", "time_sec": "1512227586", "time_usec": "151992", "timestamp": 1512227586, "capture_id": 0, "capture_ip": "127.0.0.1", "payload_len": 292, "correlation_id": ""}

protocol_header: {"type": "ip", "vlan": 0, "ip_proto": 17, "protocol": "hep", "ip_family": 3, "source_ip": "172.93.49.177", "timestamp": 1512227586, "source_port": 42557, "destination_ip": "8.8.8.8", "destination_port": 53}

payload: {"z": 0, "aa": false, "id": 65082, "qr": false, "ra": false, "rd": true, "tc": false, "anc": 0, "arc": 0, "nsc": 0, "qdc": 1, "opcode": 0, "rescode": 0, "questions": [{"name": "google.com", "type": 1, "class": 1}]}

raw: {"data":

"{"id":65082,"qr":false,"opcode":0,"aa":false,"tc":false,"rd":true,"ra":false,"z":0,"rescode":0,"qdc":1,"anc":0,"nsc":0,"arc":0,"questions":[{"name":"google.com","type":1,"class":1}],"protocol":"json-dns","timestamp":1512227586,"hep_protocol":53}

HEP JSON

JANUS & MEDIASOUP EVENTS : Select Data

```
mysql> select * from hep_proto_126_all_20171202 limit 1
```

id: 133

gid: 10

create_date: 2017-12-02 15:21:15

hep_header: {"proto": 126, "version": "3", "protocol": "hep", "time_sec": "1512222320", "time_usec": "136075", "timestamp": 1512222320, "capture_id": 0, "capture_ip": "127.0.0.1", "payload_len": 244, "correlation_id": ""}

protocol_header: {"type": "ip", "vlan": 0, "ip_proto": 17, "protocol": "hep", "ip_family": 3, "source_ip": "10.93.49.177", "timestamp": 1512222320, "source_port": 8080, "destination_ip": "10.93.100.1", "destination_port": 8080}

payload: { "type": 2, "timestamp": 1499105804472212, "session_id": "715597540605813", "handle_id": 8796940787397620, "event": { "name": "attached", "plugin": "janus.plugin.videoroom", "opaque_id": "videoroomtest-MamUvDmUymu84N_" }}



```
mysql> select * from hep_proto_133_all_20171202 limit 1
```

id: 225

gid: 10

create_date: 2017-12-02 15:21:15

hep_header: {"proto": 133, "version": "3", "protocol": "hep", "time_sec": "1512222320", "time_usec": "136075", "timestamp": 1512222320, "capture_id": 0, "capture_ip": "127.0.0.1", "payload_len": 89, "correlation_id": ""}

protocol_header: {"type": "ip", "vlan": 0, "ip_proto": 17, "protocol": "hep", "ip_family": 3, "source_ip": "10.0.0.1", "timestamp": 1512222320, "source_port": 8080, "destination_ip": "10.0.0.2", "destination_port": 8080}

payload: {"roomId":19501821,"event":"room.newpeer","peerName":"5jqagpr3","timestamp":1517502063613}



HEP JSON

HEP JSON SIP : Table Structure

```
mysql> show create table hep_proto_101_all_20171126\G
***** 1. row *****
Table: hep_proto_101_all_20171126
Create Table: CREATE TABLE `hep_proto_101_all_20171126` (
  `id` bigint(20) unsigned NOT NULL AUTO_INCREMENT,
  `gid` smallint(5) unsigned NOT NULL DEFAULT '0',
  `create_date` timestamp NOT NULL DEFAULT '1970-01-01 00:00:01',
  `hep_header` json NOT NULL,
  `protocol_header` json NOT NULL,
  `payload` json NOT NULL,
  `raw` varchar(2000) NOT NULL,
  `callid_virtual` varchar(255) GENERATED ALWAYS AS (json_unquote(json_extract(`payload`, '$.callid'))) VIRTUAL NOT NULL,
  PRIMARY KEY (`id`,`create_date`),
  KEY `create_date` (`create_date`),
  KEY `payload_callid_idx` (`callid_virtual`)
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=utf8 ROW_FORMAT=COMPRESSED
/*150100 PARTITION BY RANGE ( UNIX_TIMESTAMP(`create_date`))
(PARTITION pmax VALUES LESS THAN MAXVALUE ENGINE = InnoDB) */
```


HEP JSON

JSON SIP : Select Data

```
select * from hep_proto_1_call_20171201 limit 1\G
```

```
***** 1. row *****
```

```
id: 156
```

```
gid: 10
```

```
create_date: 2017-12-01 06:27:40
```

```
hep_header: {"proto": 1, "version": "4294967295", "protocol": "hep", "time_sec": "1512109660", "time_usec": "187", "timestamp": 1512109660,
"capture_id": 0, "capture_ip": "192.168.1.1", "payload_len": 648, "correlation_id": ""}
```

```
protocol_header: {"type": "ip", "vlan": 0, "ip_proto": 0, "protocol": "hep", "ip_family": 3, "source_ip": "192.168.1.1", "timestamp": 1512109660,
"source_port": 5060, "destination_ip": "192.168.1.2", "destination_port": 5060}
```

```
payload: {"cseq": "1", "ruri": "sip:nodejs@127.0.0.1", "via_1": "SIP/2.0/UDP
127.0.0.1:48495;branch=z9hG4bK9b82aa8fb4c7705466a3456dff7f384333332", "callid": "jhnzl3xlrg7hx0jmx529@127.0.0.1", "method": "INVITE",
"to_user": "nodejs", "from_tag": "2628881569", "protocol": "sip", "from_user": "nodejs", "ruri_user": "nodejs", "timestamp": 1512109660, "to_domain":
"127.0.0.1", "user_agent": "HEPGEN-UAC", "callid_aleg": "jhnzl3xlrg7hx0jmx529@127.0.0.1", "from_domain": "127.0.0.1", "ruri_domain": "127.0.0.1",
"transaction": "call", "content_type": "application/sdp", "hep_protocol": 1, , "via_1_branch": "z9hG4bK9b82aa8fb4c7705466a3456dff7f384333332"}
```

```
callid_virtual: jhnzl3xlrg7hx0jmx529@127.0.0.1
```

```
raw: INVITE sip:nodejs@127.0.0.1 SIP/2.0
```

```
.....
```

AWESOME!
WHAT ABOUT STATISTICS?



HOMER METRIC

HOMER SEVEN ships with a brand new modular configuration style, with every function neatly structured in blocks ready to assemble and combine, providing easy access to understand, extend and customize core logic elements.

From the main homer.cfg users can control



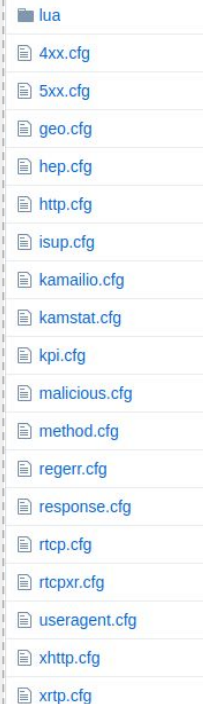
- Parameters for Homer
- Parameters for HEP Sockets
- Parameters for Data Storage
- Parameters for Elastic, Graylog, InfluxDB
- Function Switches for Time Series
- Custom Functions and Integrations

Docker Container w/ Full Stack:
<https://github.com/lmangani/homer-metric-all>

```
/* Parameters for InfluxDB */
#!substdef "!!INFLUXDB_HTTP_URL!http://192.168.2.1:8086!g"
#!substdef "!!INFLUXDB_DB!homer!g"
#!substdef "!!INFLUXDB_PRECISION!u!g"
#!substdef "!!INFLUXDB_RETENTION!autogen!g"

/* Parameters for the rtimer module sending stats */
#!substdef "!!CHECK_STATS_INTERVAL!1!g"

/* Series Selection for emission */
##!define DO_ELASTICSEARCH
#!define DO_INFLUXDB
##!define DO_GRAYLOG
#!define DO_GEO
##!define DO_ISUP
#!define DO_KPI
##!define DO_MALICIOUS
##!define DO_METHOD
##!define DO_RESPONSE
##!define DO_RTCPIXR
##!define DO_USERAGENT
##!define DO_XHTTP
#!define DO_XRTP
```





HOMER METRIC

InfluxDB

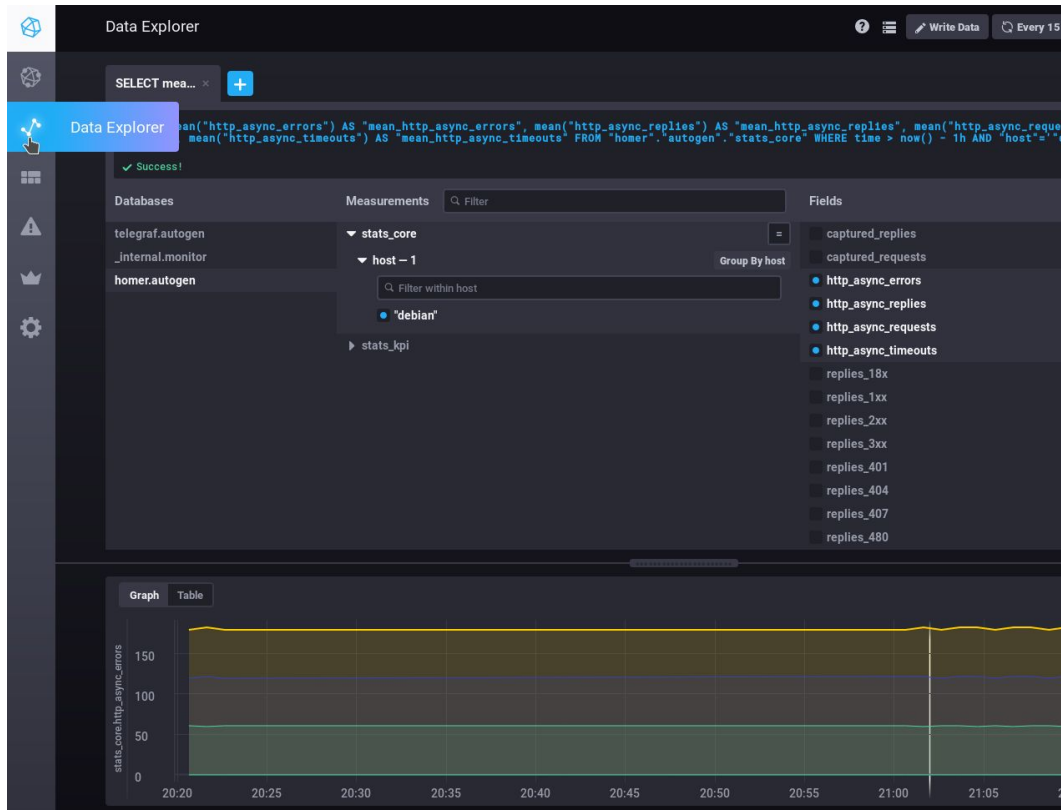
InfluxDB is a fast growing, and fast performing time series database part of the **TICK** stack, providing also Data Visualization and Alerting.

In this example we will send KPIs, Geo and X RTP Metrics every second to InfluxDB:

```
/* Parameters for InfluxDB */
#!substdef
"!INFLUXDB_HTTP_URL!http://192.168.2.1:8086!g"
#!substdef "!INFLUXDB_DB!homer!g"
#!substdef "!INFLUXDB_PRECISION!u!g"
#!substdef "!INFLUXDB_RETENTION!autogen!g"

/* Parameters for the rtimer module. */
#!substdef "!CHECK_STATS_INTERVAL!1!g"
```

Exported data can instantly be leveraged using tools such as **Grafana**, **Chronograf**, **Kapacitor**



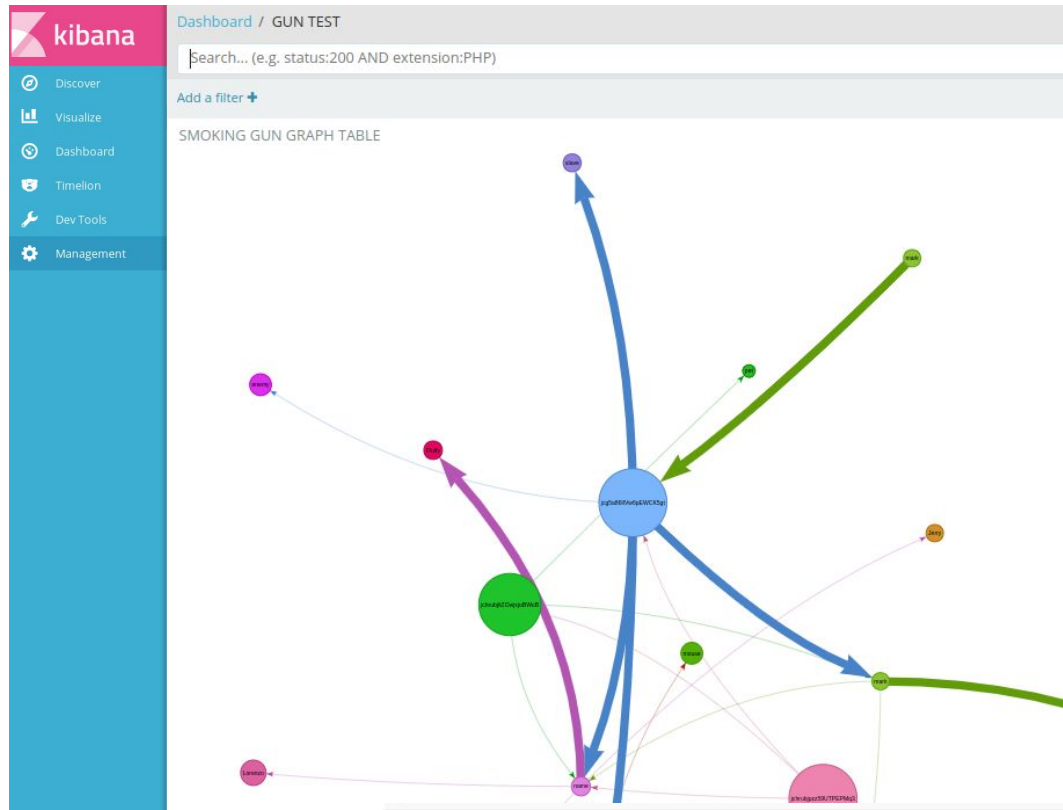


Elasticsearch is a very popular and powerful full-text search-engine based on Lucene and part of the **ELK** stack alongside **Kibana** and **Logstash**.

In this example we will send KPIs, Geo and X RTP Metrics every second to Elasticsearch:

```
/* Parameters for Elasticsearch */
#!/substdef "!"ELASTICSEARCH_HTTP_URL!http://127.0.0.1:9200!g"
#!/define DO ELASTICSEARCH
```

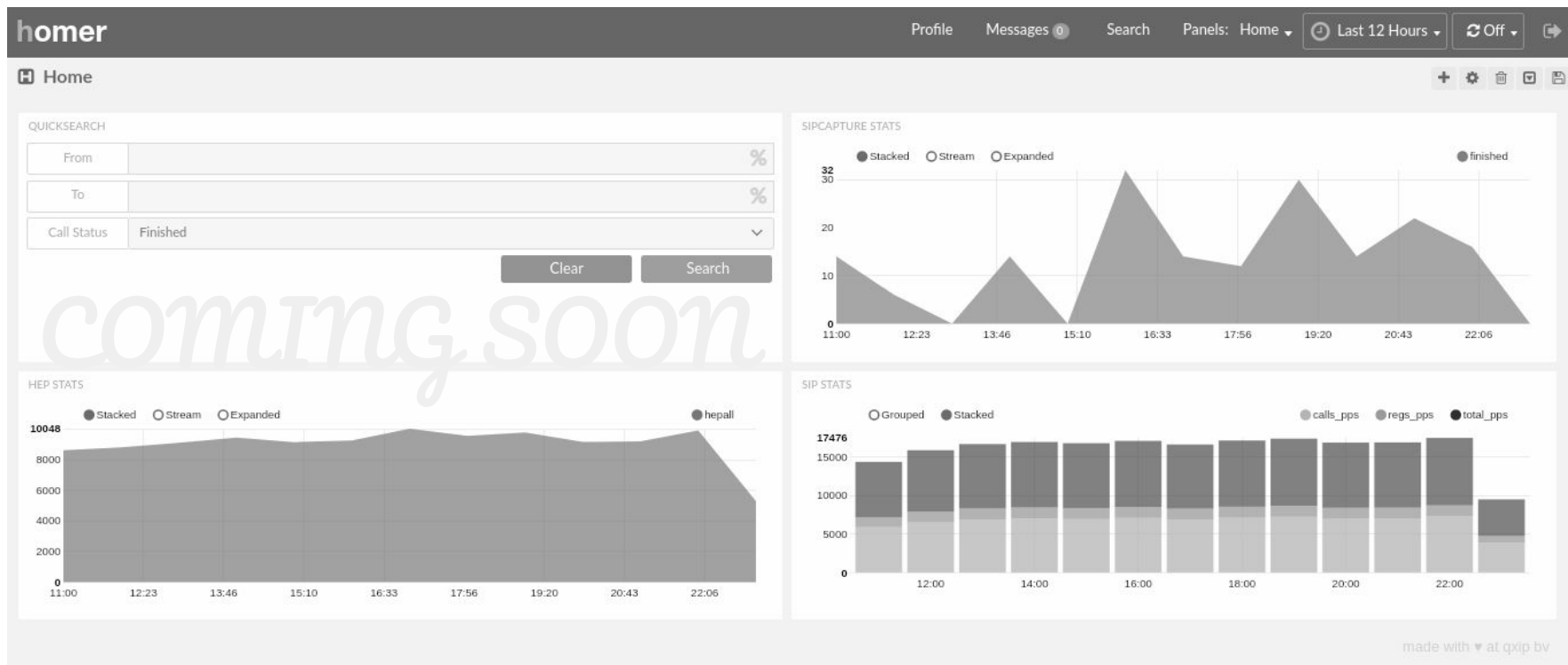
Exported data can instantly be leveraged using tools such as **Kibana** and alerted with our dedicated FOSS Kibana plugin **SENTINL**





HOMER UI

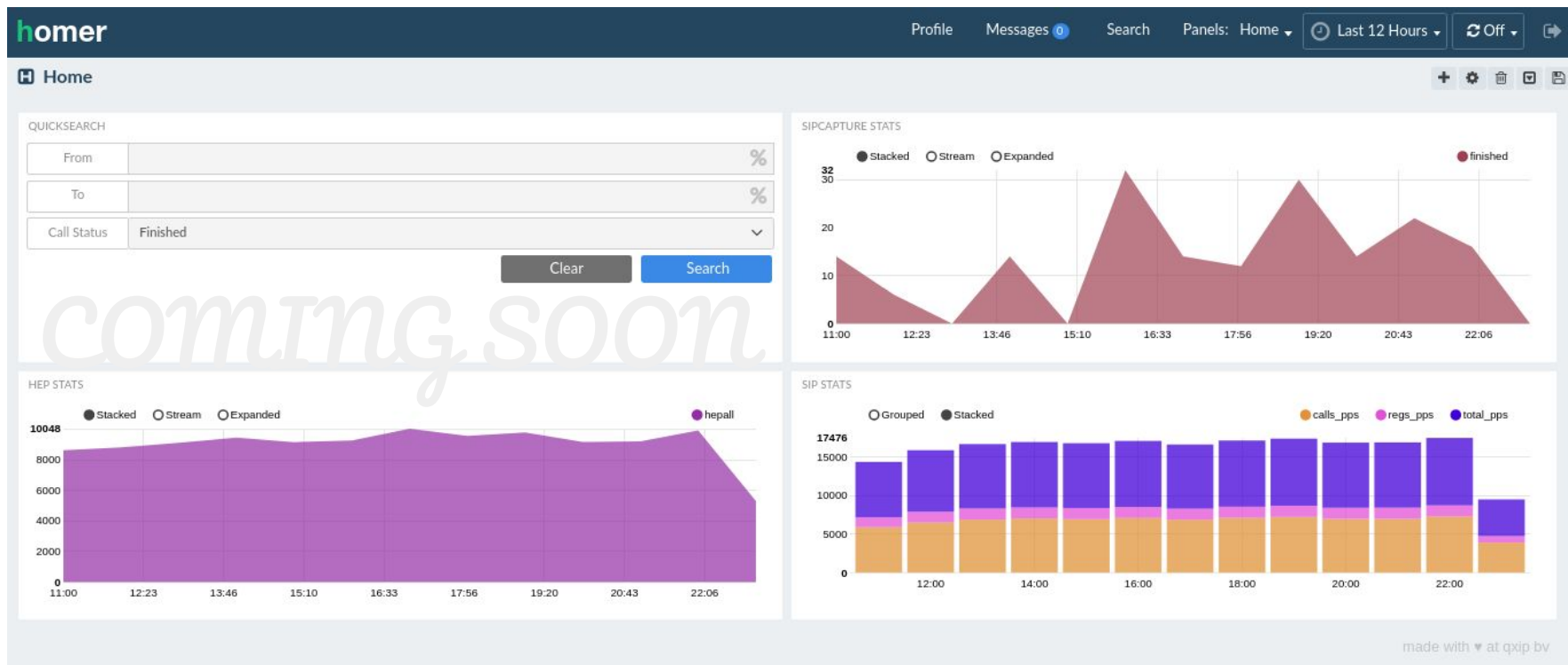
*Ladies and Gentlemen, meet our last kidney stone - once completed, **HOMER Seven** will be usable!*





HOMER UI

*Ladies and Gentlemen, meet our last kidney stone - once completed, **HOMER Seven** will be usable!*



"That's all Folks!"



Time's UP! Thanks for attending our Flash Talk!
Got Questions? Come and ask Us (almost) anything!

Please do help us by supporting the **HOMER** project!
PS: Testing, Documenting, and Promoting are as valuable as Coding

SIPCAPTURE @GITHUB	http://sipcapture.org + http://sipcapture.io
HOMER @GITHUB	http://github.com/sipcapture/homer
HEPIC @WEBSITE	http://hepic.tel
MAILING-LIST @USERS	https://groups.google.com/forum/#!forum/homer-discuss