ESPRESSO EDITION

meet #HOMER

@FOSDEM 2016

Written by:

Alexandr Dubovikov, Lorenzo Mangani

HOMER Development Team

http://sipcapture.org

Sponsored by QXIP BV - http://qxip.net

Quick Introduction to **QXIP** and **SIPCAPTURE**

ABOUT US

QXIP *{QuickSIP}* is an Dutch R&D Company specializing in Open-Source and Commercial Voice Technology Development

SIPCAPTURE is an Open-Source foundation and community primarily sponsored by QXIP BV and its Founders

Our flagship OSS projects is SIPCAPTURE **HOMER** based on our mature and open encapsulation protocol **HEP/EEP**

Our Open-Source and Commercial solutions are deployed and trusted by thousands of Businesses worldwide.

Our Customers include large telephony network operators, voice service carriers, voip service providers, cloud service providers, call center operators, voice equipment vendors and Enterprises relying on VoIP including Fortune 500

Our Capture Technologies are natively implemented in all major OSS voip platforms such as *Kamailio, OpenSIPS, FreeSWITCH, Asterisk, OpenUC* and many capture tools such as *sipgrep*, *sngrep, our captagent* and more.

Our Github repository at http://github.com/sipcapture features all of our software and many **HEP** integration examples.

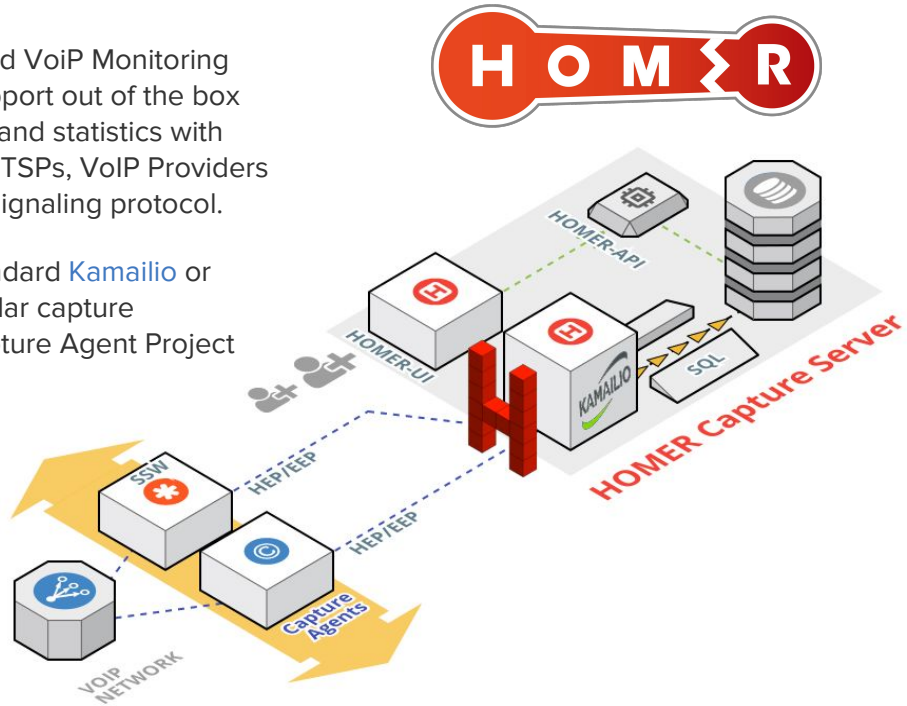
For full details abour our projects and services please visit our website at http://qxip.net

SIPCAPTURE + HOMER

100% Open Source VoIP Monitoring and Troubleshooting Tools

HOMER is a robust, carrier-grade, scalable SIP Capture system and VoiP Monitoring Application offering HEP/EEP, IPIP & port mirroring/monitoring support out of the box ready to process, index & store insane amounts of signaling, logs and statistics with instant search, end-to-end analysis and drill-down capabilities for ITSPs, VoIP Providers Trunk Suppliers as well as Enterprises and Developers using SIP signaling protocol.

Powered at the core by our SIPCAPTURE Module for industry-standard Kamailio or OpenSIPS, **HOMER** provides a virtually unlimited scope for granular capture configuration either stand-alone or using our companion **HEP** Capture Agent Project



HOMER provides many features and advantages, including:

- Instant centralized access to present and past signaling & stats
- Full SIP/SDP payload with precise timestamping
- Automatic correlation of sessions, logs and reports
- Visual representation of multi session call-flows
- Fast detection of usage and system anomalies
- System agnostic view of VoIP traffic flows
- Unlimited plug & play capture agents and HEP data feeds
- Multi-User and Customizable UI based on JS/Angular/D3
- Exporting and Sharing functionality built-in... and much more!

FIND ALL ABOUT HOMER: http://github.com/sipcapture/homer

HOMER: Capture Architecture

Capture Server vs. Capture Agents

HEP BLOCKS

A typical **HOMER** setup is composed of two basic elements/blocks:

HEP CS: CAPTURE AGENT

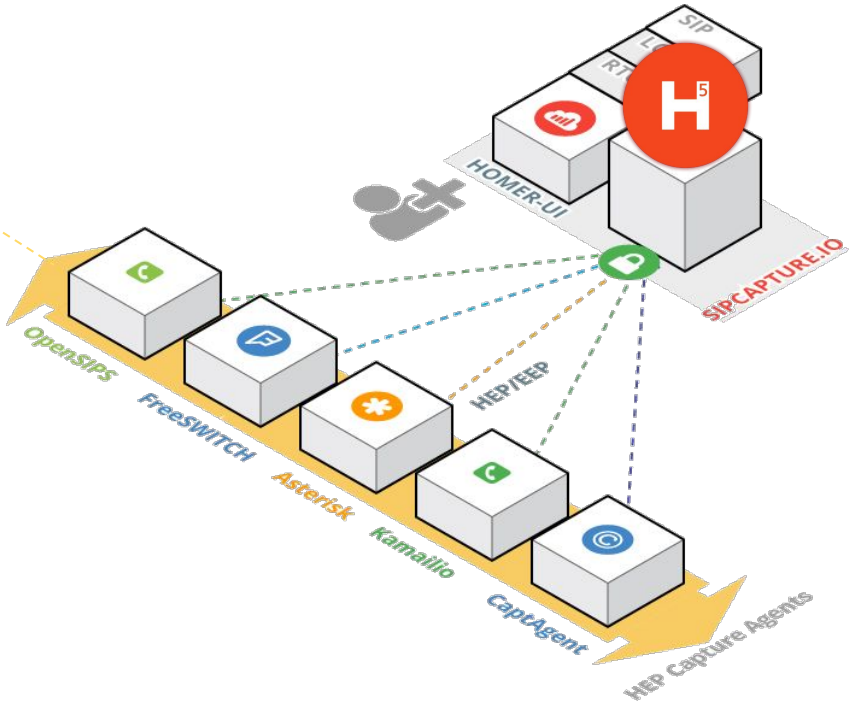
The Capture Agent captures and sends encapsulated network packets or json data to a Capture Server using the *HEP/EEP* Encapsulation protocol

The Capture Agent role can be covered by multiple elements running on different platforms and distributed in a completely modular fashion, easy to scale, grow and expand alongside the monitored infrastructure and systems, allowing flexible support for any network topology including cloud scenarios.

HEP CA: CAPTURE SERVER

The *Capture Server Collects, Indexes and Stores* to Database network packets received from *Capture Agents* or Captured via local RAW Sockets

The capture server supports *HEP v1/2/3*, *IPIP, JSON Payloads* encapsulation delivered by Agents or captured from interfaces and mirrored switch ports, using flexible rules defined in the powerful, extensible and customizable core capture plan.



HOMER 5: What is HEP/EEP?

HEP = Homer Encapsulation Protocol

HEP/EEP

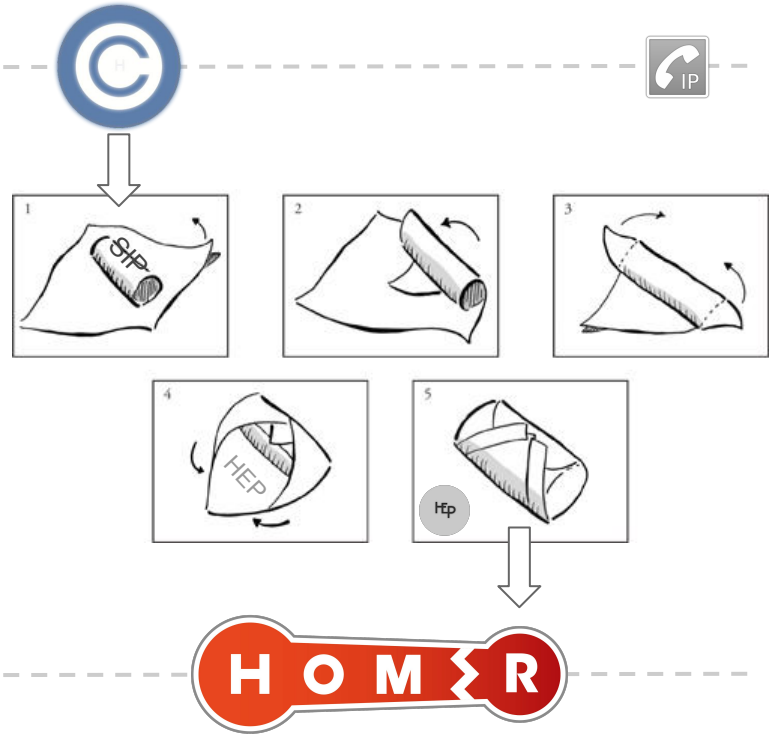
HOMER's Encapsulation protocol *(HEP/EEP)* is the building block used to wrap and transfer captured packets between a capture Agent and Server.

The HEP Extensible Encapsulation protocol was designed to provide an efficient, modular and low -level framework to accurately duplicate passively obtained IP datagrams for remote collection over *UDP/TCP/SCTP* connections, where full retention of original datagram headers and payload MUST be provided to the collector without alterations or data loss.

The *HEP3/EEP* definition includes both generic *(internal)* and vendor- specific custom defined chunk types providing ground for implementors to extend the spectrum of the deliverable data within the HEP protocol alongside the encapsulated IP datagram.

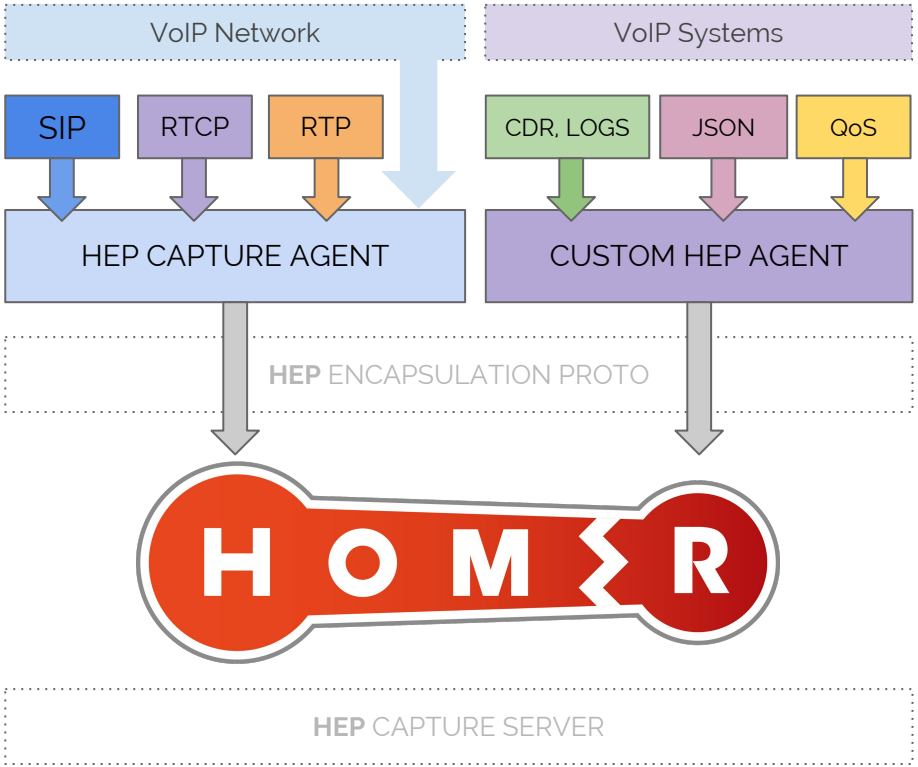
HOMER currently supports HEP decoding for *SIP, XMPP, RTCP, RTCP-XR* and *Custom Logs* or *CDRs* in plain text or *JSON* format.

Find the full HEP/EEP specs at: http://github.com/sipcapture/hep

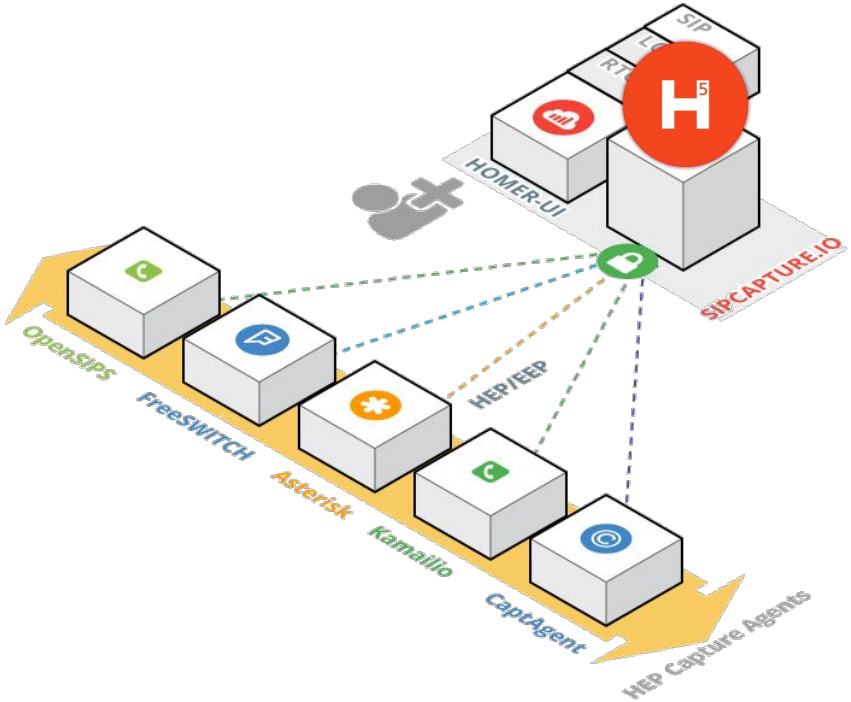


HOMER 5: How does it work?

Build your own HOMER Capture Server using SIPCAPTURE modules



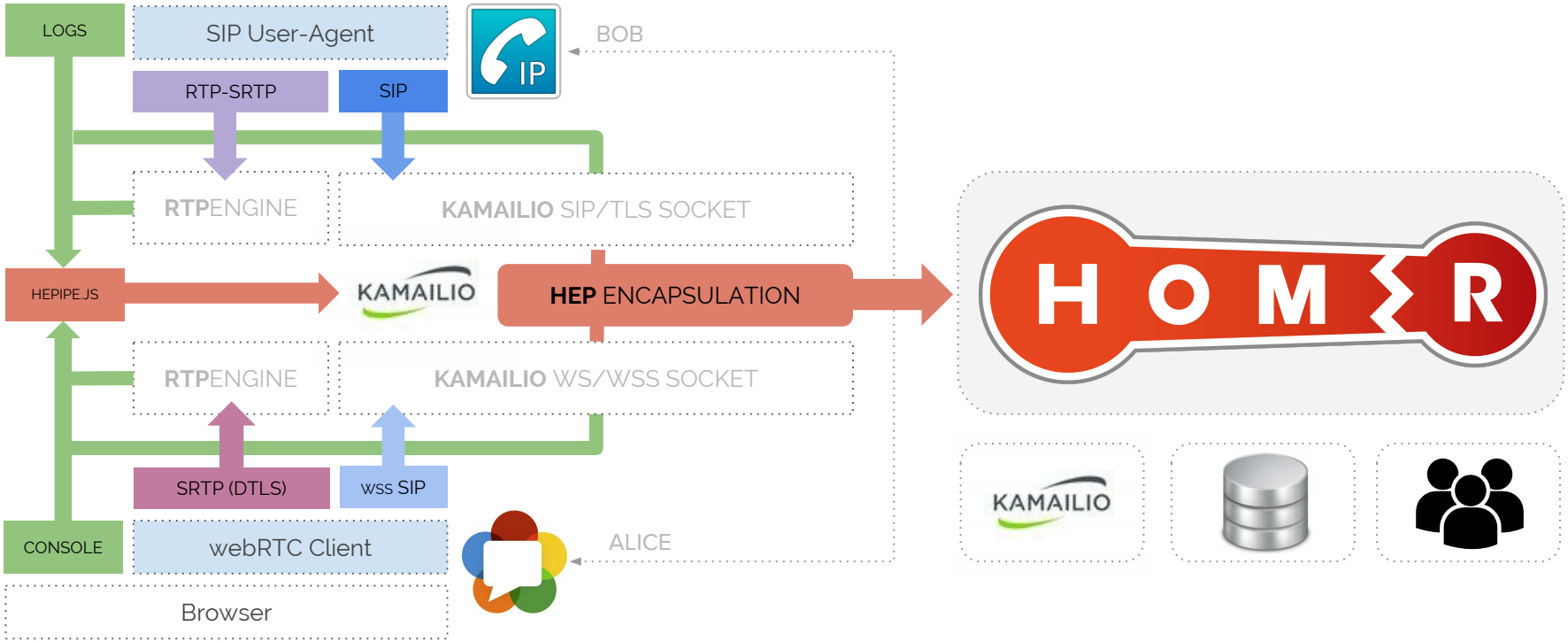
HEP AGENTS



HOMER 5: webRTC Capture

Capture SIP + WebRTC using Kamailio Logs + Hepipe.js

WebRTC

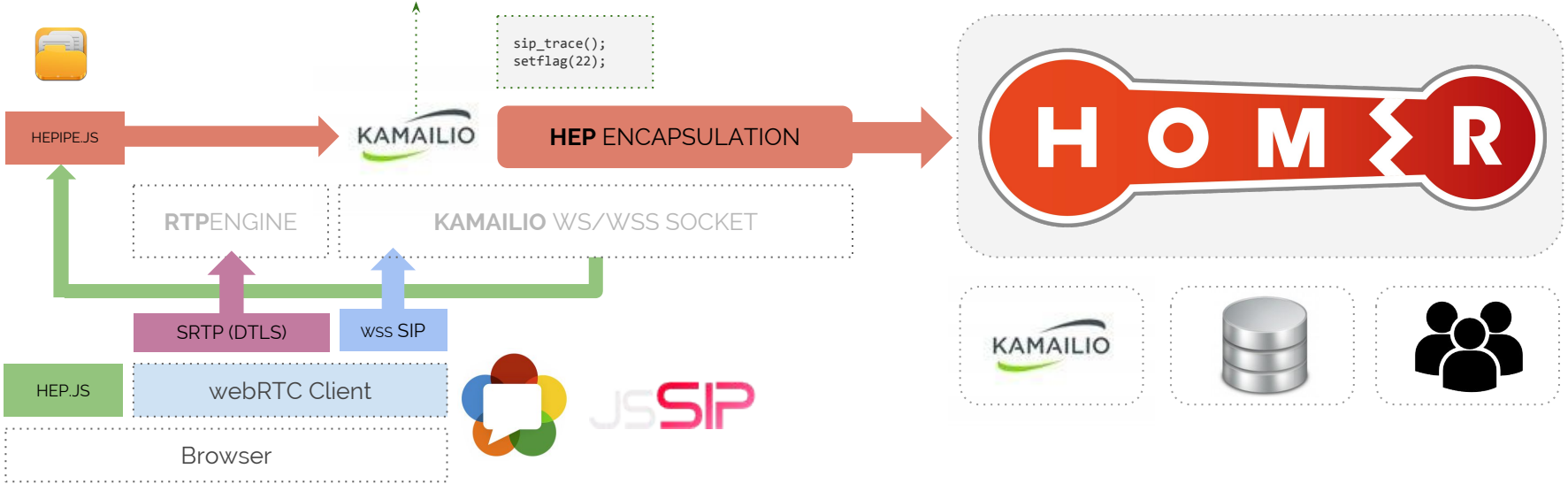


HOMER 5: webRTC Capture

http://github.com/sipcapture/wiki

Javascript

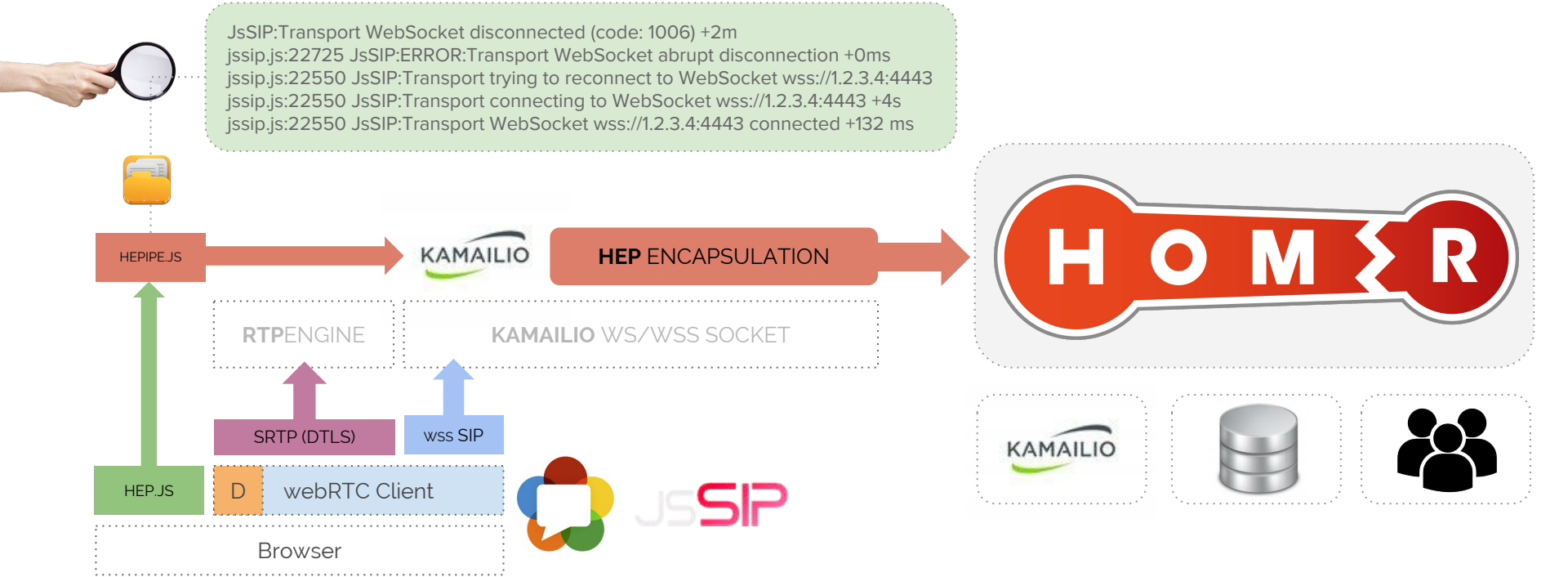
```
if (proto == WS || proto == WSS) {
  setflag(SRC_WS);

  xlog("L_INFO", "homerwss CID: [$ci], SIP: Method: $rm, CSEQ: $cs, RU: $rU, WSS Request: RM: $var(wss_rm), RU: $var(wss_ru),
       UAC: $var(wss_uac), Connection: $var(wss_connection), Upgrade: $var(wss_upgrade), Origin: $var(wss_origin),
       Host: $var(wss_host), Sec_Proto: $var(wss_sec_proto), Sec-Key: $var(wss_sec_key), WS_VERSION: $var(wss_sec_version)");
}
```



HOMER 5: Javascript/Node.JS HEP

http://github.com/sipcapture/hepipe-js

Javascript



HOMER 5: WSS Call Flow

WSS to SIP Call Troubleshooting

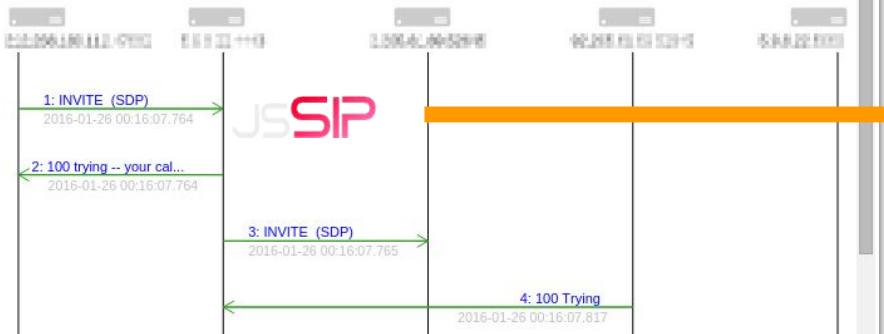
SIP/WSS

SIP Signaling | Search

Id	Date	Method	Reason	RURI user	From User	To User	CallID	CallID_AL	User Age..	Source H..	SPort	Destinati..	DPort	Pr..	Node
304	2016-01-26 00:16:15.671	200	OK		201	101	4dar0hqpfkfm8o5q0b4q			[redacted]	52645	[redacted]	4443	3	homer01:...
306	2016-01-26 00:16:15.672	200	OK		201	101	4dar0hqpfkfm8o5q0b4q			[redacted]	4443	[redacted]	47682	3	homer01:...
307	2016-01-26 00:16:15.718	ACK		lq1pna1u	201	101	4dar0hqpfkfm8o5q0b4q		JsSIP 0.7....	[redacted]	47682	[redacted]	4443	3	homer01:...
308	2016-01-26 00:16:22.192	BYE		lq1pna1u	201	101	4dar0hqpfkfm8o5q0b4q		JsSIP 0.7....	[redacted]	47682	[redacted]	4443	3	homer01:...
309	2016-01-26 00:16:22.192	BYE		lq1pna1u	201	101	4dar0hqpfkfm8o5q0b4q		JsSIP 0.7....	[redacted]	5060	[redacted]	52645	3	homer01:...
310	2016-01-26 00:16:22.258	200	OK		201	101	4dar0hqpfkfm8o5q0b4q			[redacted]	52645	[redacted]	4443	3	homer01:...
311	2016-01-26 00:16:22.259	200	OK		201	101	4dar0hqpfkfm8o5q0b4q			[redacted]	4443	[redacted]	47682	3	homer01:...

Call-ID: 4dar0hqpfkfm8o5q0b4q

Call-Flow | QoS Reports | Logs | Export | Session Duration: 00:00:15.495



Call-ID: 4dar0hqpfkfm8o5q0b4q

Call-Flow | QoS Reports | Logs | Export | Session Duration: 00:00:15.495

Filter Logs

Jan 26 00:16:07 de2 /usr/local/kamailio-dev/sbin/kamailio[30724]: INFO: <script>: homerwss CID: [4dar0hqpfkfm8o5q0b4q], SIP: Method: INVITE, CSEQ: 2592, RU: 101, WSS Request: RM: GET, RU: GET, UAC Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.82 Safari/ Connection: Upgrade, Upgrade: websocket, Origin: https://qxip.net, Host: [redacted]:4443, Sec_Proto: sip, Sec-Key /DVdxELiK/RSckW2qnVntQ==, WS_VERSION: 13

Jan 26 00:16:15 de2 /usr/local/kamailio-dev/sbin/kamailio[30723]: INFO: <script>: homerwss CID: [4dar0hqpfkfm8o5q0b4q], SIP: Method: ACK, CSEQ: 2592, RU: lq1pna1u, WSS Request: RM: GET, RU: GET, U Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.106 Safari/537.36, Connection: Upgrade, Upgrade: websocket, Origin: https://www.qxip.net, Host: [redacted]:4443, Sec_Proto: sip, Se KgmB8o/jekG74S2v3wEl8Q==, WS_VERSION: 13

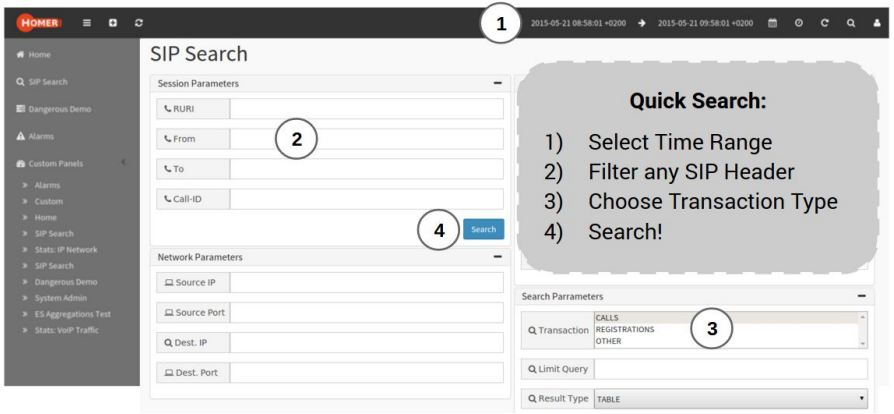
HOMER 5: Dashboards and Widgets

Build your own Troubleshooting Environment

UI

HOMER provides powerful search and indexing features to easily locate and retrieve sessions using time-range, transaction type and standard or custom header matching using fully customizable user forms.

HOMER search results can be further filtered and refined client-side to reduce database hits and optimize daily workflows. All correlated reports and logs are automatically included when a session is selected and can be easily exported and shared.



Id	Date	Method	Reason	RURI user	From User	To User	CallID	CallID_AL	User Agent	Source Host	SPo.	Destination	DPo.	Pr.	Node
12866	2015-11-25 18:01:19.000	200	Alive		nodejs	nodejs	hd1i1he61or@127.0.0.1			192.168.1.2	5060	192.168.1.1	5060	1	homer01:0
12867	2015-11-25 18:03:10.000	OPTIONS			nodejs	nodejs	byv67irizfr@127.0.0.1		SIPCAPTUR...	192.168.1.1	5060	192.168.1.2	5060	1	homer01:0
12868	2015-11-25 18:03:10.000	200	Alive		nodejs	nodejs	byv67irizfr@127.0.0.1			192.168.1.2	5060	192.168.1.1	5060	1	homer01:0
12869	2015-11-25 18:13:07.000	OPTIONS			nodejs	nodejs	cemcu6usor@127.0.0.1		SIPCAPTUR...	192.168.1.1	5060	192.168.1.2	5060	1	homer01:0
12870	2015-11-25 18:13:07.000	200	Alive		nodejs	nodejs	cemcu6usor@127.0.0.1			192.168.1.2	5060	192.168.1.1	5060	1	homer01:0
12871	2015-11-25 18:31:08.000	OPTIONS			nodejs	nodejs	dskrgkl0udi@127.0.0.1		SIPCAPTUR...	192.168.1.1	5060	192.168.1.2	5060	1	homer01:0
12872	2015-11-25 18:31:08.000	200	Alive		nodejs	nodejs	dskrgkl0udi@127.0.0.1			192.168.1.2	5060	192.168.1.1	5060	1	homer01:0
12873	2015-11-25 18:47:07.000	OPTIONS			nodejs	nodejs	22jjd04fgvi@127.0.0.1		SIPCAPTUR...	192.168.1.1	5060	192.168.1.2	5060	1	homer01:0
12874	2015-11-25 18:47:07.000	200	Alive		nodejs	nodejs	22jjd04fgvi@127.0.0.1			192.168.1.2	5060	192.168.1.1	5060	1	homer01:0

HOMER 5: Dashboards and Widgets

Build your own Troubleshooting Environment

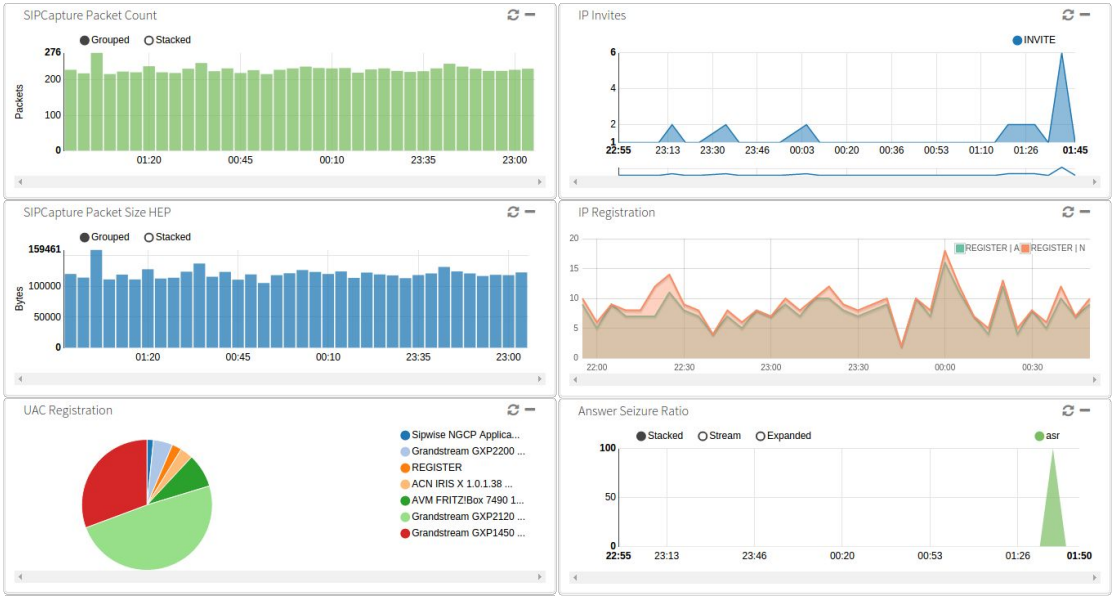
UI

HOMER can generate a virtually unlimited number of user customizable statistics and metrics on its monitored traffic and sessions.

All statistics are immediately available and can be easily displayed using the included wizard using a growing number of widgets covering charting, data tables and mapping of internal database tables and external data sources.

All widgets and functions are synchronized to the global time-range selector with user cache and preferences for continuous utilization.

TLDR; Tons of Customizable Charts
(D3, Highcharts, Flot and more!)



Interested? Try HOMER 5 in 5 minutes

SIPCAPTURE public *Homer-Docker* image

DOCKER

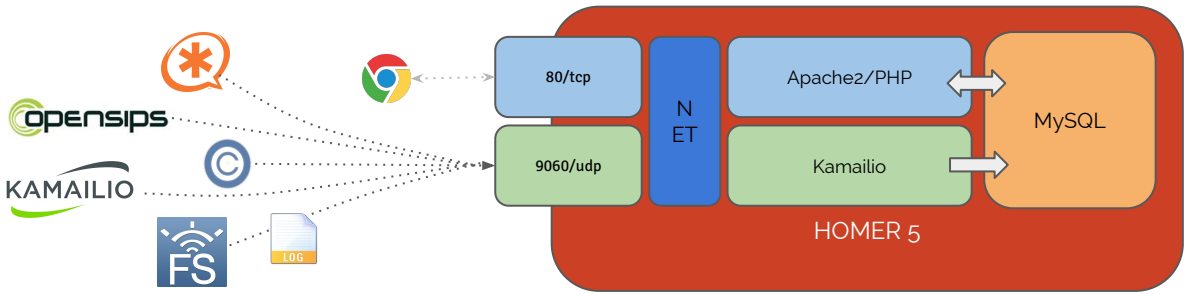
Download and run the **Homer 5** application bundle *[Apache2-PHP/MySQL-InnoDB/Kamailio-sipcapture]*

```
# docker run -tid --name homer5 -p 80:80 -p 9060:9060/udp qxip/homer-docker
4280d228ae472c02eded508bf587fb0bde6bd1604b1fc65c0490d0648f6fbe06
```

Verify the **Homer 5** container is running and all desired ports are published:

```
# docker ps
CONTAINER ID   IMAGE              COMMAND    CREATED       STATUS        PORTS              NAMES
4280d228ae47   qxip/homer-docker  "/run.sh"  1 minute ago  Up 1 minutes  80/tcp,9060/udp    0c0f7939-5ab9-401e-af63-ce8728221d0b-n1/homer5
```

Start sending HEP traffic to your container using your favourite *HEP/EEP* Capture Agent:

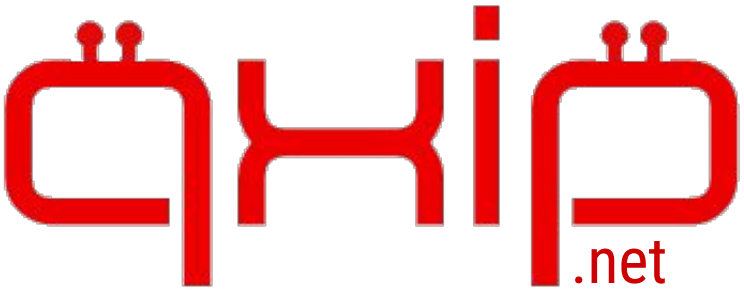


... it's that simple!

"Thats all Folks!"

Time's UP! Want to go further? "HEP" Yourself!

SIPCAPTURE @GITHUB	http://sipcapture.org + http://sipcapture.io
HOMER @GITHUB	http://github.com/sipcapture/homer
CAPTAGENT @GITHUB	http://github.com/sipcapture/captagent
HEPIPE.JS @GITHUB	http://github.com/sipcapture/hepipe.js
MAILING-LIST @USERS	https://groups.google.com/forum/#!forum/homer-discuss


.net