Homer VoIP Monitoring
From zero to hero

Workshop - Kamailio World 2017
Giacomo Vacca
@giavac

About me

I design, develop and maintain RTC platforms based on Open Source applications since 2001.

Using Kamailio since it was still OpenSER as core component for fixed, mobile and WebRTC services (Truphone, Libon, Nexmo and many others).

Currently owner of RTCSoft (rtcsoft.net), member of sipcapture team, RTC Architect at Nexmo

@giavac - https://github.com/giavac

Interact in real time during the workshop

The Homer team is available **now** at

https://gitter.im/sipcapture/home

Introduction

The need for Homer - VoIP Monitoring and Troubleshooting

- Understand **exactly** what happened in your platform, analysing specific calls or events.
  - Search through a massive amount of collected data
  - Born with a *SIP-centric* view, then evolved (and still evolving) towards QoS, RTCP, logs and custom events.
- Homer is already integrated with the most successful Open Source RTC applications (Kamailio, OpenSIPS, FreeSWITCH, Asterisk, RTPEngine, Janus).
- Homer can be used in other cases too (with **captagent**, sngrep, hepipe.js).

Key Features

- Open Source, modular
- Easy to deploy in various scenarios
- Easy to extend/adapt
  - This is how many become contributors
- Very high performances, with a clear scaling strategy
- Carrier grade networks but also smaller deployments
  - Can be useful during development
- Hosted *vs* Cloud
  - http://sipcapture.org/#cloud

The ecosystem - native support

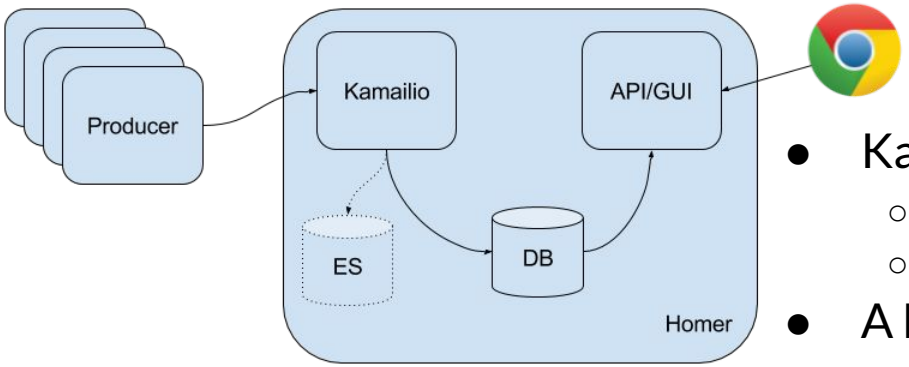
- A dedicated binary protocol: **HEP**
  - https://github.com/sipcapture/HEP/blob/master/docs/HEP3_rev12.pdf
  - Wireshark dissector: https://github.com/sipcapture/hep-wireshark
- OSS apps native support
  - Kamailio (***siptrace, sipcapture***)
  - OpenSIPS (***siptrace, sipcapture, proto_hep***)
  - FreeSWITCH (***sofia***)
  - Asterisk (***res_hep***)
  - RTPEngine (--*homer*=...)
  - sngrep

The ecosystem - external support

- External support
  - Janus (via events plugin)
  - FreeSWITCH for non-SIP events (via ESL)
  - captagent for any other need (including ERSPAN encapsulation)
  - sngrep
- Libraries in various languages
  - C
  - Java
  - JS
  - Go
  - Perl
  - Python
  - Erlang

Architecture

Main Architectural Components



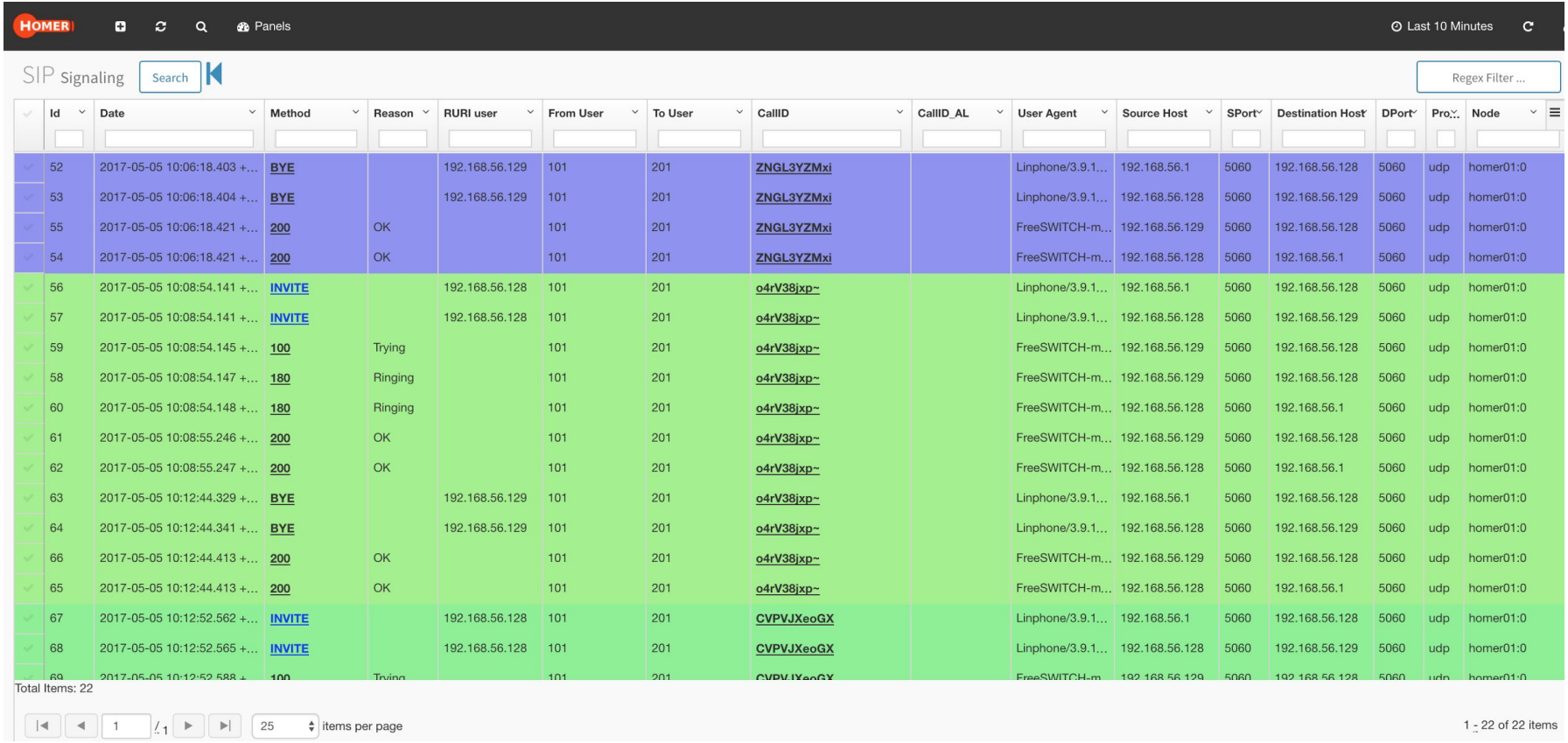
- Kamailio: a high-performance collector of data
  - Store in DB
  - Send to ElasticSearch
- A **DB**: mysql/postgres
- An **API** (PHP-based, easy to debug and extend)
  - https://github.com/sipcapture/homer-api
- A **GUI** (Angular) and web server (nginx, apache)
  - https://github.com/sipcapture/homer-ui

Data

- SIP signalling
- RTCP (and RTCP-XR) reports
- Logs
- End of call QoS reports
- WebRTC
- ISUP
- Periodic QoS reports from RTPAgent

Call Info

- Full SIP/SDP storage with precise timestamps
- RTCP reports
- Custom events/logs correlated to call flows
- Multiple-legs correlation
  - Need to carry other leg's Call ID in custom SIP header

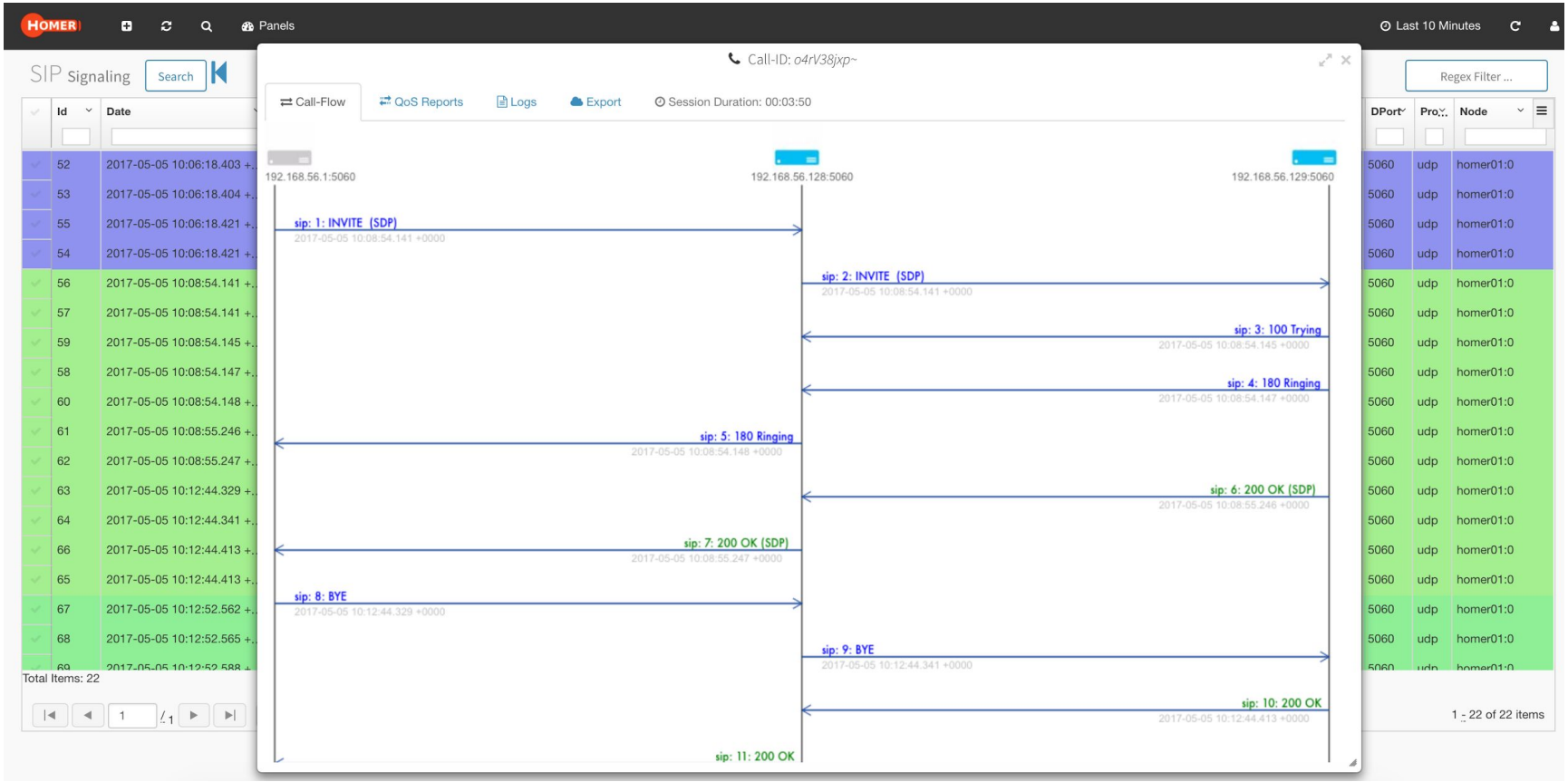


Id	Date	Method	Reason	RURI user	From User	To User	CallID	CallID_AL	User Agent	Source Host	SPort	Destination Host	DPort	Pro..	Node
52	2017-05-05 10:06:18.403 +...	BYE		192.168.56.129	101	201	ZNGL3YZMxi		Linphone/3.9.1...	192.168.56.1	5060	192.168.56.128	5060	udp	homer01:0
53	2017-05-05 10:06:18.404 +...	BYE		192.168.56.129	101	201	ZNGL3YZMxi		Linphone/3.9.1...	192.168.56.128	5060	192.168.56.129	5060	udp	homer01:0
55	2017-05-05 10:06:18.421 +...	200	OK		101	201	ZNGL3YZMxi		FreeSWITCH-m...	192.168.56.129	5060	192.168.56.128	5060	udp	homer01:0
54	2017-05-05 10:06:18.421 +...	200	OK		101	201	ZNGL3YZMxi		FreeSWITCH-m...	192.168.56.128	5060	192.168.56.1	5060	udp	homer01:0
56	2017-05-05 10:08:54.141 +...	INVITE		192.168.56.128	101	201	o4rV38jxp~		Linphone/3.9.1...	192.168.56.1	5060	192.168.56.128	5060	udp	homer01:0
57	2017-05-05 10:08:54.141 +...	INVITE		192.168.56.128	101	201	o4rV38jxp~		Linphone/3.9.1...	192.168.56.128	5060	192.168.56.129	5060	udp	homer01:0
59	2017-05-05 10:08:54.145 +...	100	Trying		101	201	o4rV38jxp~		FreeSWITCH-m...	192.168.56.129	5060	192.168.56.128	5060	udp	homer01:0
58	2017-05-05 10:08:54.147 +...	180	Ringing		101	201	o4rV38jxp~		FreeSWITCH-m...	192.168.56.129	5060	192.168.56.128	5060	udp	homer01:0
60	2017-05-05 10:08:54.148 +...	180	Ringing		101	201	o4rV38jxp~		FreeSWITCH-m...	192.168.56.128	5060	192.168.56.1	5060	udp	homer01:0
61	2017-05-05 10:08:55.246 +...	200	OK		101	201	o4rV38jxp~		FreeSWITCH-m...	192.168.56.129	5060	192.168.56.128	5060	udp	homer01:0
62	2017-05-05 10:08:55.247 +...	200	OK		101	201	o4rV38jxp~		FreeSWITCH-m...	192.168.56.128	5060	192.168.56.1	5060	udp	homer01:0
63	2017-05-05 10:12:44.329 +...	BYE		192.168.56.129	101	201	o4rV38jxp~		Linphone/3.9.1...	192.168.56.1	5060	192.168.56.128	5060	udp	homer01:0
64	2017-05-05 10:12:44.341 +...	BYE		192.168.56.129	101	201	o4rV38jxp~		Linphone/3.9.1...	192.168.56.128	5060	192.168.56.129	5060	udp	homer01:0
66	2017-05-05 10:12:44.413 +...	200	OK		101	201	o4rV38jxp~		FreeSWITCH-m...	192.168.56.129	5060	192.168.56.128	5060	udp	homer01:0
65	2017-05-05 10:12:44.413 +...	200	OK		101	201	o4rV38jxp~		FreeSWITCH-m...	192.168.56.128	5060	192.168.56.1	5060	udp	homer01:0
67	2017-05-05 10:12:52.562 +...	INVITE		192.168.56.128	101	201	CVPVJXeoGX		Linphone/3.9.1...	192.168.56.1	5060	192.168.56.128	5060	udp	homer01:0
68	2017-05-05 10:12:52.565 +...	INVITE		192.168.56.128	101	201	CVPVJXeoGX		Linphone/3.9.1...	192.168.56.128	5060	192.168.56.129	5060	udp	homer01:0
69	2017-05-05 10:12:52.588 +...	100	Trying		101	201	CVPVJXeoGX		FreeSWITCH-m...	192.168.56.129	5060	192.168.56.128	5060	udp	homer01:0

A search result with packet list and details

Call Flows

- One key feature: Correlation of separate SIP legs into one “call”
  - Use custom SIP headers to carry info on other legs’ Call IDs



A simple call flow

Collaboration Tools

Call flows can be shared by:

- Extracting pcaps
- Extracting PNGs
- Sharing a link

This is where collaborative debugging really gets a boost

Customizations - examples

```
#!ifdef WITH_HOMER_DEST_STATS

    route(PARSE_DEST_STATS);

#!endif
```

- Stats on SIP error codes per country
  - Needs a custom SIP header (*P-Dest-Stats*) from producers
- ASR/ACD per destination/source IP/group
- ASR/ACD per component
- Define your own stats and alarms

The Key Role of Kamailio

- Receive and decode HEP data
  - With kamailio 5: *nonsip_hook* and *event_route[sipcapture:request]*
- Write on DB
- Generate statistics
- Custom statistics
- Optionally GeoIP details
- Can transmit data to ElasticSearch

Homer kamailio.cfg 1/2

```
#!substdef "!HOMER_DB_USER!homer!g"

#!substdef "!HOMER_DB_PASSWORD!homer_password!g"

#!substdef "!HOMER_LISTEN_PROTO!udp!g"

#!substdef "!HOMER_LISTEN_IF!0.0.0.0!g"

#!substdef "!HOMER_LISTEN_PORT!9060!g"

…

listen=HOMER_LISTEN_PROTO:HOMER_LISTEN_IF:HOMER_LISTEN_PORT

…

sip_capture($var(dest_table));
```

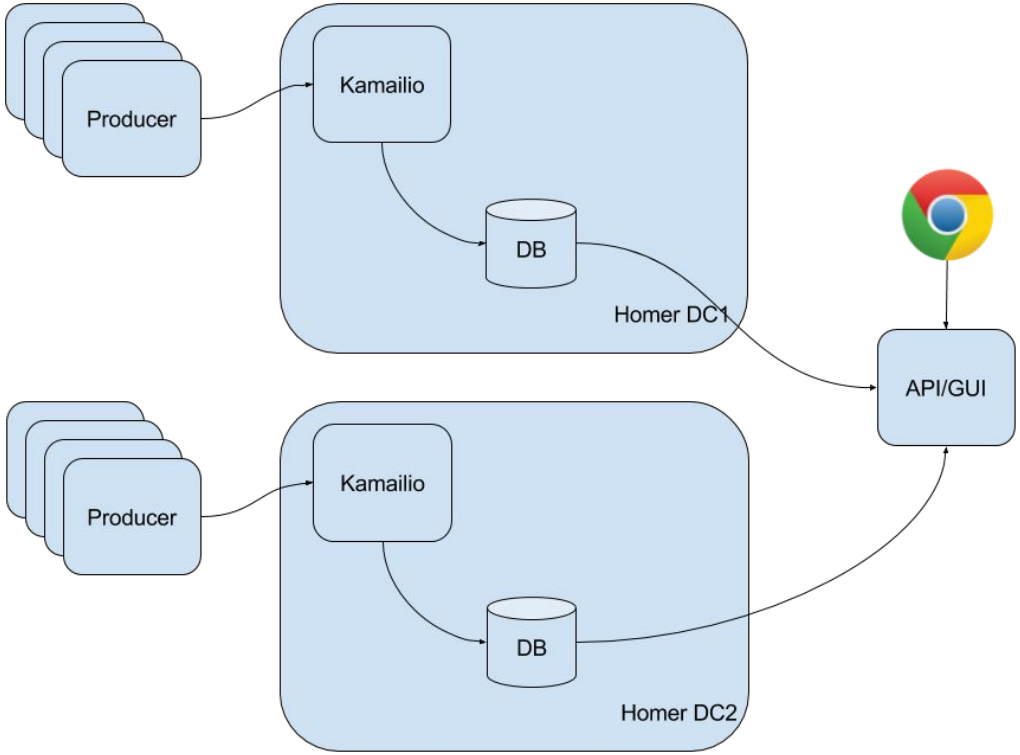
Homer kamailio.cfg 2/2

```
modparam("sipcapture", "db_url", "mysql://HOMER_DB_USER:HOMER_DB_PASSWORD@127.0.0.1/homer_data")

modparam("sipcapture", "capture_on", 1)

modparam("sipcapture", "hep_capture_on", 1)

modparam("sipcapture", "insert_retries", 5)

modparam("sipcapture", "insert_retry_timeout", 10)
```

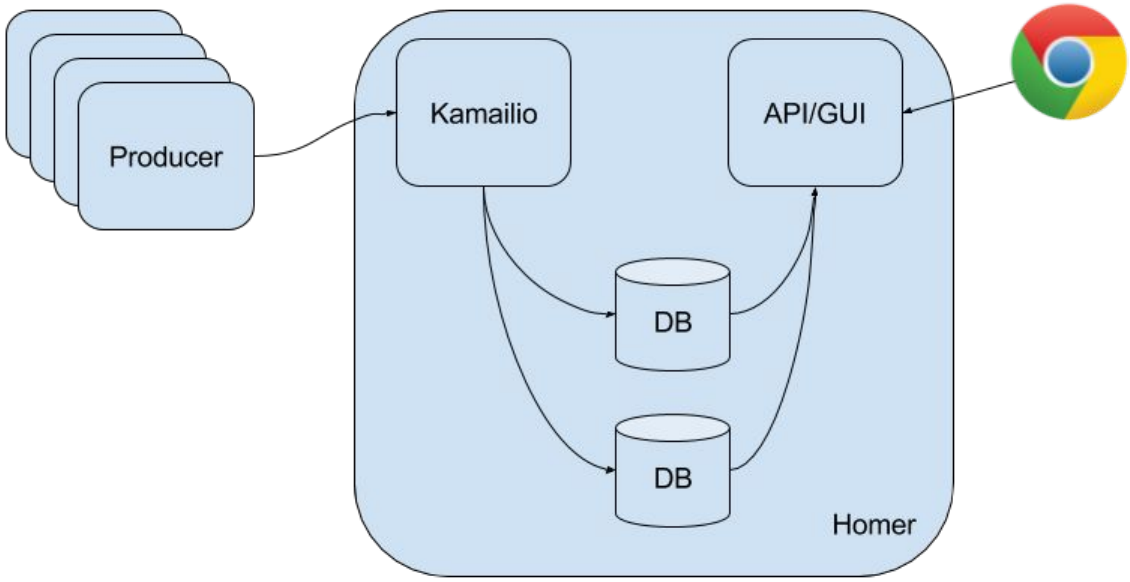
Multi-node And Scaling

- Write rate is the bottleneck
  - Kamailio is a key component for fast writes
  - Sharding by method or Call ID
  - Distribute writes across multiple mysql instances
    - Sharding upported by **siptrace** module and **captagent**
- Producers of data in separate data centres
  - Keep the data local when possible
- Reads can be performed across several nodes
  - Acceptable to be much slower than writes
- Other approaches
  - UDP-level load balancing

Distribution across Data Centres



Sharding



Deployments

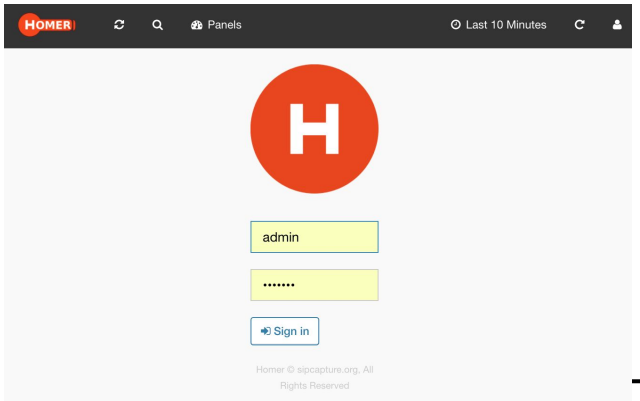
Installation Strategies

- Bash script
- Docker
  - Single and Multi-Container
  - Suitable for Kubernetes & Co.
- Puppet
  - Master/Slave
  - Standalone
  - To manage Docker containers
- Custom
  - Often the DB installation and setup is delegated to a DBA team

A Minimalistic Installation

- Homer can fit into one single host
  - Useful for small deployments and development
- https://github.com/sipcapture/homer-installer
  - Debian 8 and CentOS 7

```
bash <( curl -s https://cdn.rawgit.com/sipcapture/homer-installer/master/homer_installer.sh )
```



Default credentials: admin/test123

Docker Installation

https://github.com/sipcapture/homer-docker

- Based on Docker Compose
- One container for all or...
- One container per service
  - Kamailio
  - mysql
  - API/Web
  - An additional container for dashboard persistence
- Integrates well with external DBs
  - `USE_REMOTE_MYSQL=true` in *homer.env*

Containers in action

- git clone https://github.com/sipcapture/homer-docker.git
- cd homer-docker
- docker-compose build
- docker-compose up -d
- docker ps

Puppet module

- Debian, Ubuntu, CentOS
  - small elements changing, e.g. PHP version and installation paths
- See also “pre-install” bash script for max automation
- Various parameters
  - mysql management is optional
- Can manage a Docker-based installation via Compose

https://github.com/sipcapture/homer-puppet

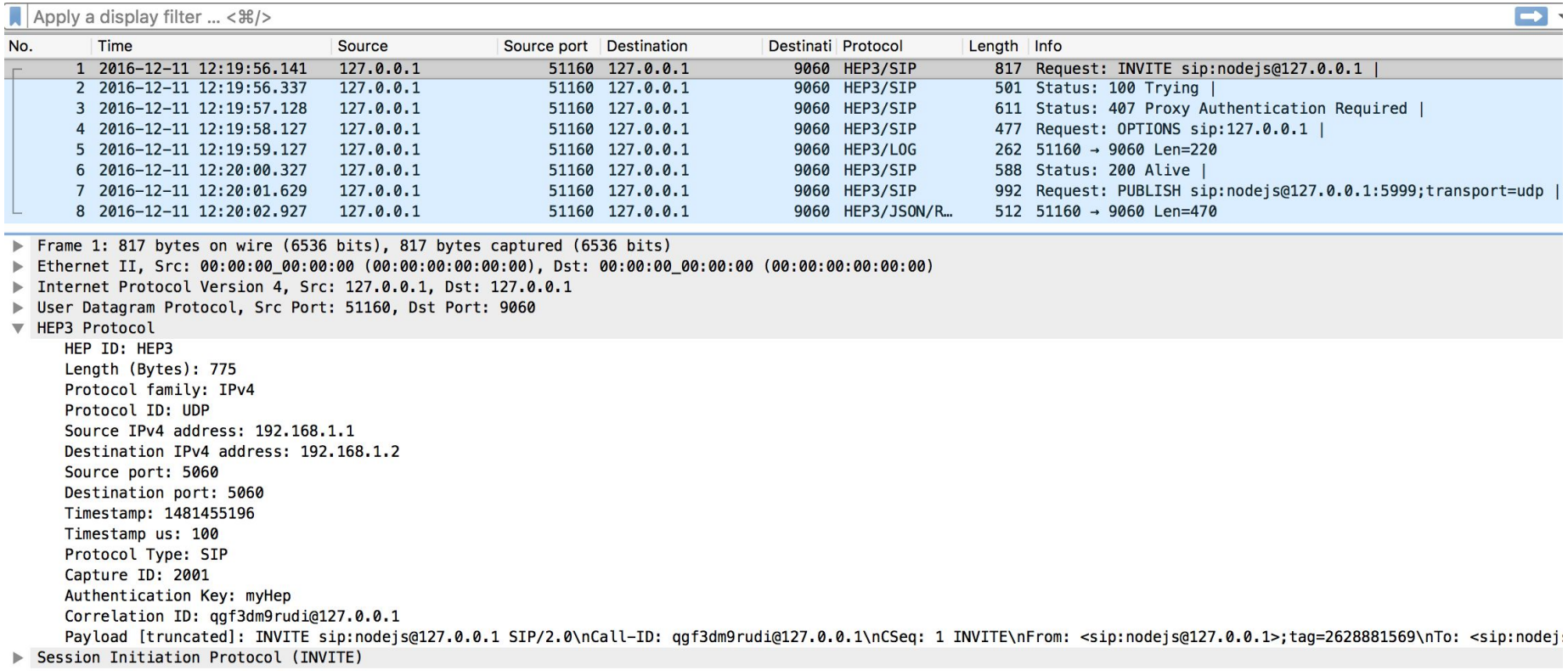
```
node default {

  class { 'homer':

    manage_mysql   => false,

    mysql_host     => '10.0.0.10',

    Mysql_password => 'da_mysql_pass',

  }

}
```

More

Debugging The... Debugging Tool

- hepgen.js
  - https://github.com/sipcapture/hepgen.js
  - Generate HEP data to smoke-test Homer
  - A reference to learn HEP format
- Wireshark dissector
  - https://github.com/sipcapture/hep-wireshark
  - HEP with SIP, ISUP, logs, RTCP reports, and other payload types
  - **Contributions to extend to other protocols are welcome**

HEP in Wireshark



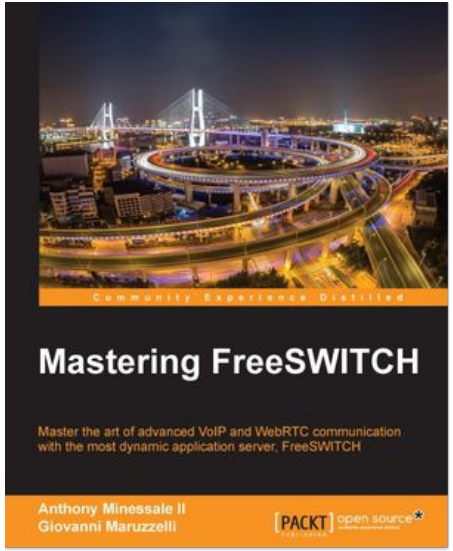
Kamailio as Producer

- Configure siptrace
  - Homer IP address and port
- Filter messages in kamailio.cfg
- With Kamailio 5 siptrace module has:
  - HEPv3 support
  - **heplog()** command to send a log item directly from the .cfg

Kamailio siptrace configuration

```
modparam("siptrace", "duplicate_uri", "sip:HOMER_IP:9060");

modparam("siptrace", "hep_mode_on", 1);

modparam("siptrace", "trace_on", 1)

modparam("siptrace", "trace_to_database", 0)

modparam("siptrace", "trace_flag", 24)

modparam("siptrace", "hep_version", 3);

…

sip_trace();

setflag(24);
```

FreeSWITCH as Producer



- Configure sofia profile
  - <param name="sip-capture" value="yes/no"/>
  - <param name="capture-server" value="udp:10.0.0.10:9060"/>
- Example with A-leg off and B-leg ON
- hepipe.js to get non-SIP events via ESL

See also "Mastering FreeSWITCH", chapter 13

https://www.packtpub.com/networking-and-servers/mastering-freeswitch

Captagent for all other cases

https://github.com/sipcapture/captagent

- Configure the tracing filters
  - SIP, ISUP, RTP reports
- Configure where Homer is located and launch

```
sudo apt-get update && apt-get install -y libexpat-dev libpcap-dev libjson0-dev libtool automake
flex bison libuv-dev make

./build.sh && ./configure && make && sudo make install

- Edit socket_pcap (/usr/local/captagent/etc/captagent/socket_pcap.xml)

- Edit transport_hep (/usr/local/captagent/etc/captagent/transport_hep.xml)
```

Wrapping up

Conclusions

- Homer is a must have for VoIP/RTC troubleshooting
- Open Source, modular, can be deployed in various ways
- The future is… **HEPIC**
  - Collect/Correlate/Graph Everything
  - **paStash**: generic-purpose nodejs correlator
  - Latest HEPIC presentation by Lorenzo: http://tinyurl.com/hepic-homer
- “RTC-TIE: Distributed Backlist for Fraud Prevention”
  - Don’t miss Alexandr’s presentation on Wednesday!

Thanks And Q&A

Questions?

Special thanks to:

Lorenzo Mangani

Alexandr Dubovikov

Federico Cabiddu

Doug Smith

@giavac for more questions later

Additional slides

Configuration

- Users
- Nodes
- Aliases
- Links to share
- Groups
- Alarms

Statistics

- Packets count
- Replies by method
- Destination replies
- IP addresses
- Geolocation
- User Agents
- ASR, NER
- Custom stats (with dedicated Stats server - ElasticSearch)

Alarms

- “Friendly” scanners
- mysql injections attempts
- Loops
- Timeouts
- etc + configurable in Homer kamailio.cfg

Data Retention Policies

- A cron job rotates mysql tables
  - Default: daily
- Only limitation is disk space
- Retention policies are configurable in *rotation.ini*
- Also configure max size of data (e.g. for large SDPs…)

QoS Info, Logs, etc

- Homer can collect RTCP reports and correlate them with the SIP signalling
- Also correlate **log lines** to SIP signalling