



Homer

... because sip capturing makes sense

author: Alexandr Dubovikov

co-authors: Torsten Schweizer, Heino Klier, Roland Haenel

QSC AG

About QSC

QSC – ICT solutions for small and mid-size enterprises

QSC AG, Cologne/Germany, is a service provider for voice and data communication, as well as the ICT services that build upon them.

Established in 1997, the company has been focusing on small and mid-size business customers.

QSC is the first provider to operate an Open Access platform, which unites a wide range of broadband technologies to offer national and international site networking, including Managed Services.

QSC additionally supplies its customers and distribution partners with a comprehensive product portfolio that can be modularly adapted to every need.

QSC was the first provider in Germany to build its own Next Generation Network (NGN), and therefore enjoys long years of experience in connection with IP-based telephony solutions, in particular.

QSC employs a workforce of some 700 people and has been listed on the TecDAX index since 2004.

Capturing tools

- Tcpdump
- Ngrep
- Sipgrep
- Wireshark
- Sipspy

All these tools are able to capture in realtime!
But we have to take a look into history!

Why do we need capturing?

Example scenario:

- A customer complains experiencing problems with reaching a special phone number. Usually, to discover the problem and locate the faulty device in the network you have to do a live trace together with the customer. But you do not want to bother him with test calls.
- This is the big benefit of HOMER!
With HOMER we are able to search for the faulty call and get results retrospectively to the call flow from every involved network device.

A trace Tool with backtrace functionality is needed:
Homer



Homer Simpson © 20th Century Fox

A trace Tool with backtrace functionality is needed:
Homer

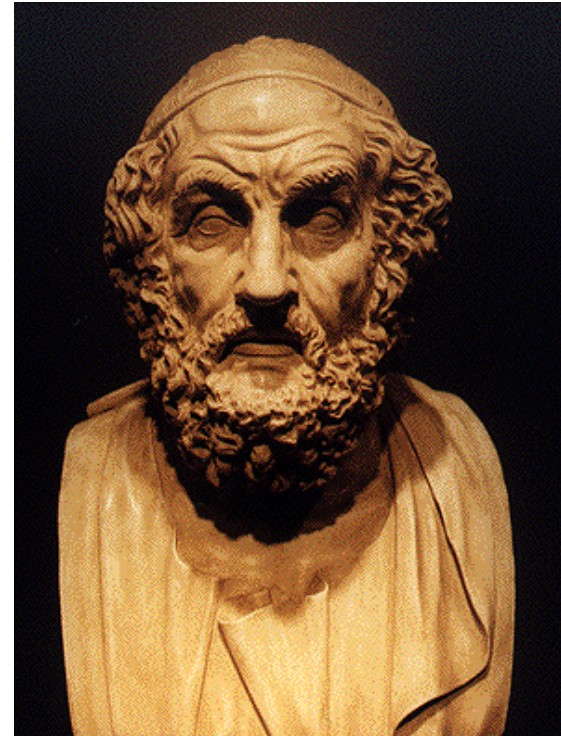


Homer Simpson © 20th Century Fox

A trace Tool with backtrace functionality is needed:
Homer



Homer Simpson © 20th Century Fox



A trace Tool with backtrace functionality is needed:
Homer

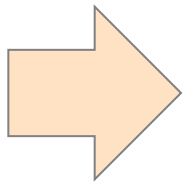


Homer Simpson © 20th Century Fox



Why HOMER?

- it collects data and captured messages
- storing the collected data in DB
- querying, filtering and displaying of data via web interface (GUI)



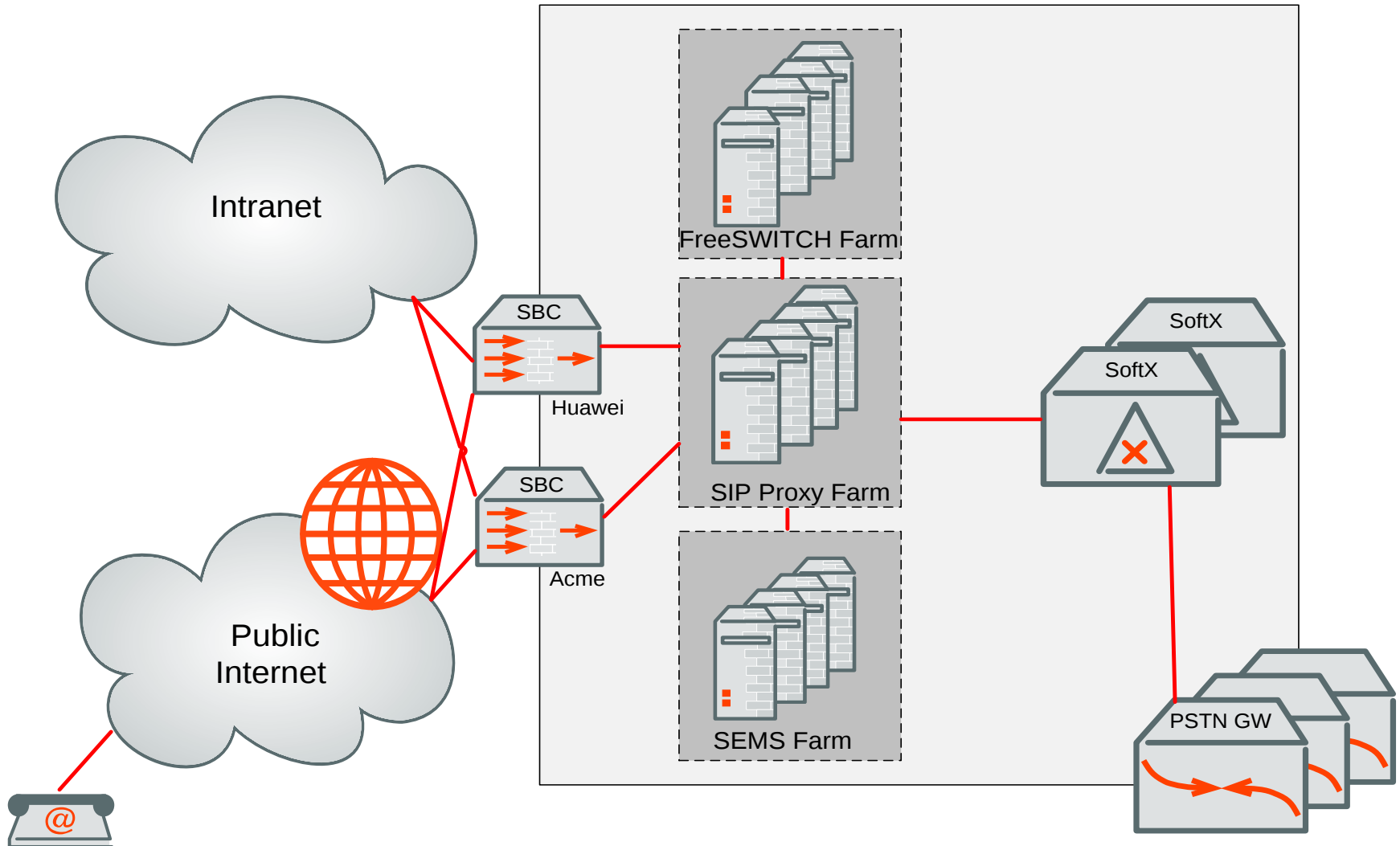
The criteria for our system!

Normal SIP/VoIP network components

- SBC (Session Border Controller)
- Softswitch/Gateway
- SIP proxy/registrar/router
- SIP media

services/voice2email/fax2email/IVR/applications

NGN Network Overview



Centralized – Vendor independent

- There are many different system components in a SIP network
- Many vendors support IP Proto 4 (IP in IP encaps) for capturing solutions, e.g. ACME Packet, Huawei ...
- Our aim is to bring all SIP components together in a centralized controlling and monitoring system
- As a result you have the complete call flow through all components of your VoIP network

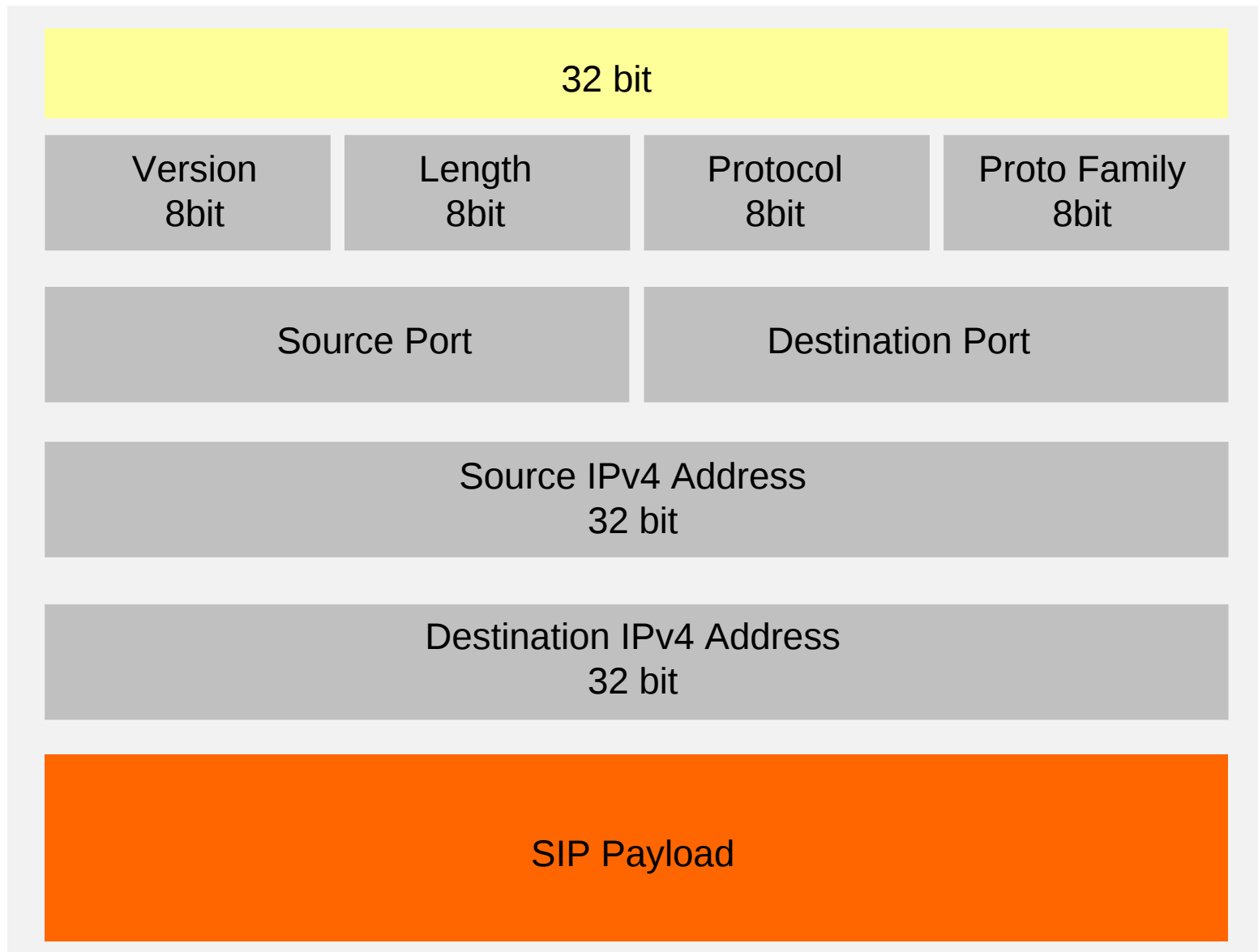
Homer is based on:

- External capturing agent (if needed)
- Capturing nodes
- Capturing database
- Web frontend (GUI)

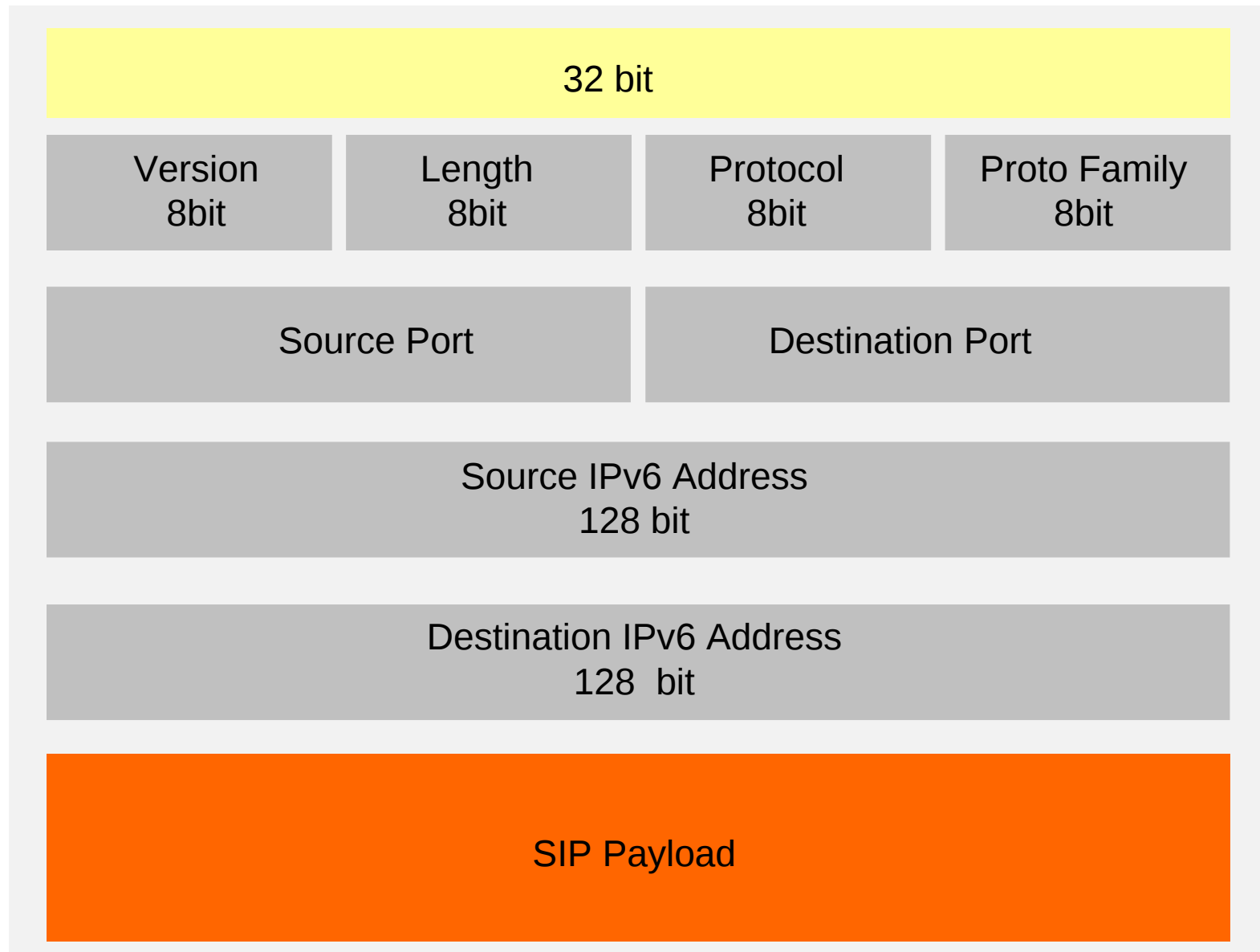
HEP - Homer Encapsulation Protocol

- self developed encapsulation protocol
- no need of root privileges or kernel changes like IP/IP
- IPv6 and IPv4
- supports many IP protocols (TCP,UDP,SCTP)
- can be used not only for SIP

HEP – Homer Encapsulated Protocol IPv4



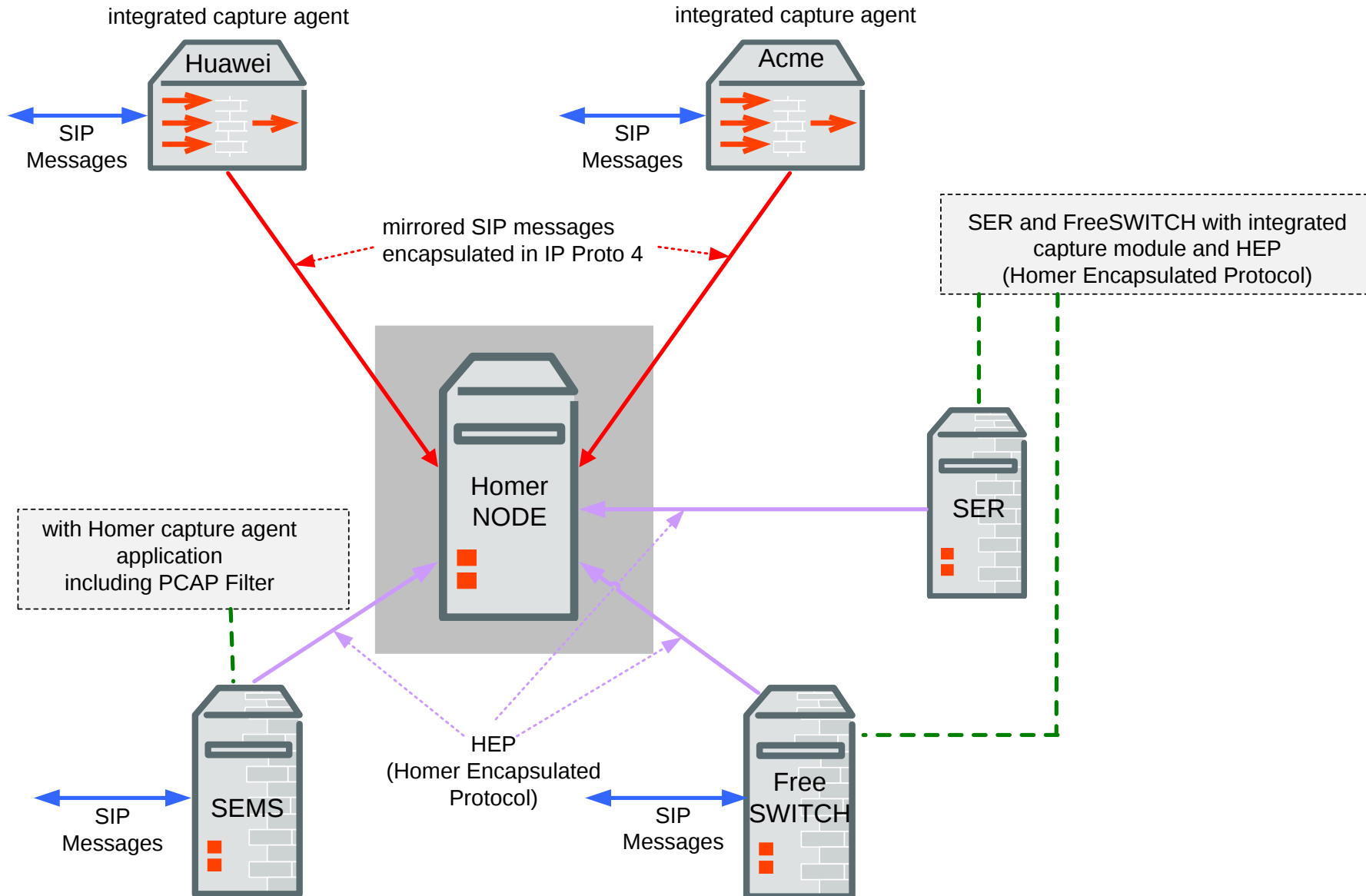
HEP – Homer Encapsulated Protocol IPv6



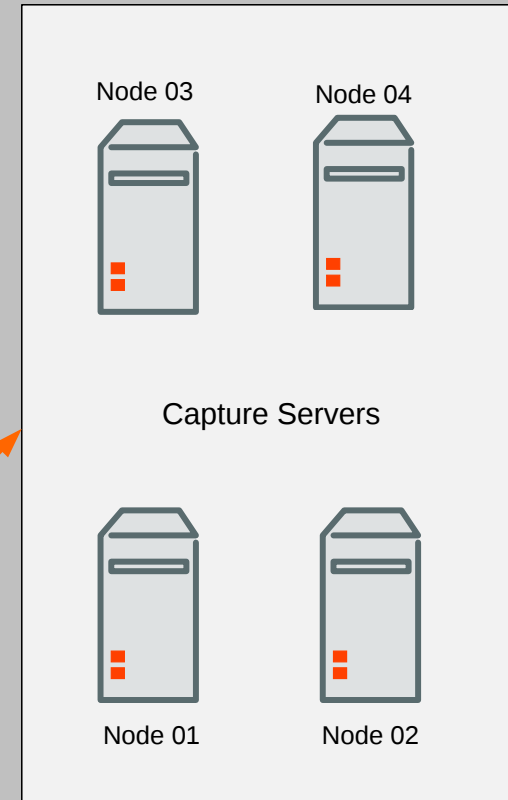
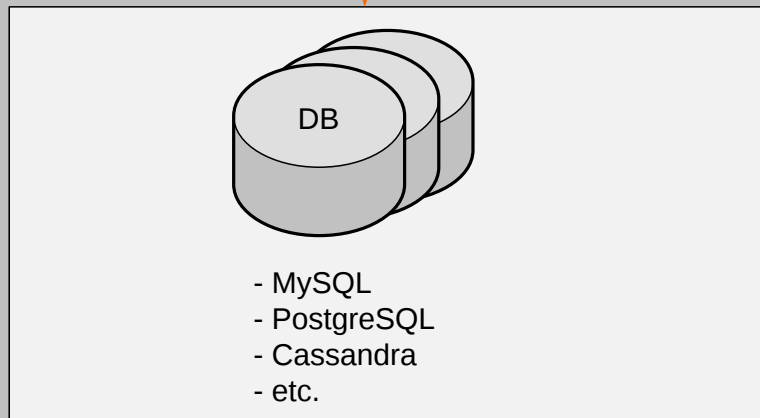
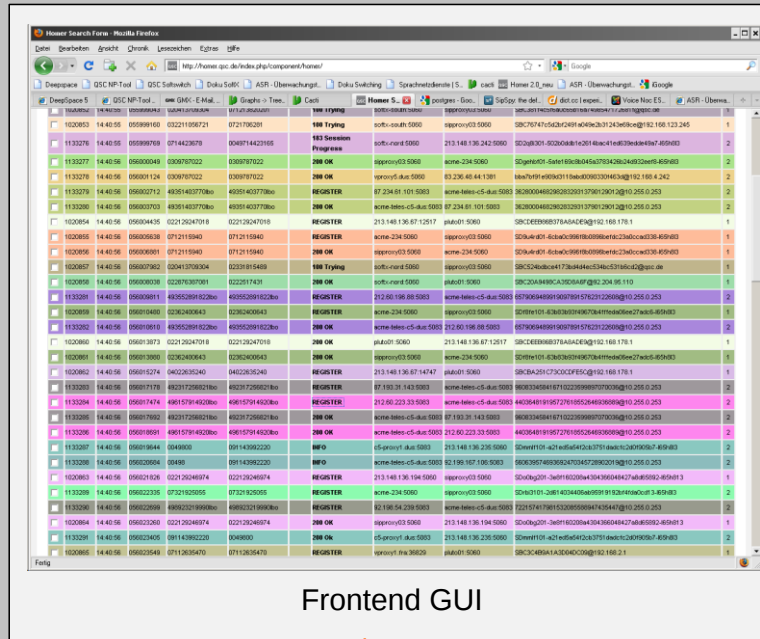
Capturing agent

- The capturing agent acts as a daemon process on operation systems like UNIX (also possible as a Windows component)
- The agent duplicates all SIP traffic in HEP to the Homer node
- The agent uses the pcap lib. Therefore you can set up your own pcap filter to duplicate only needed traffic, e.g. only outgoing messages
- The agent is extremely small, with only 300 lines of C-code and therefore goes easy on resources
- A widespread integration of the capturing agent in many other open source projects (Asterisk, Yate, OpenSIPS) would be helpful, since it is already implemented in FreeSWITCH and Kamailio

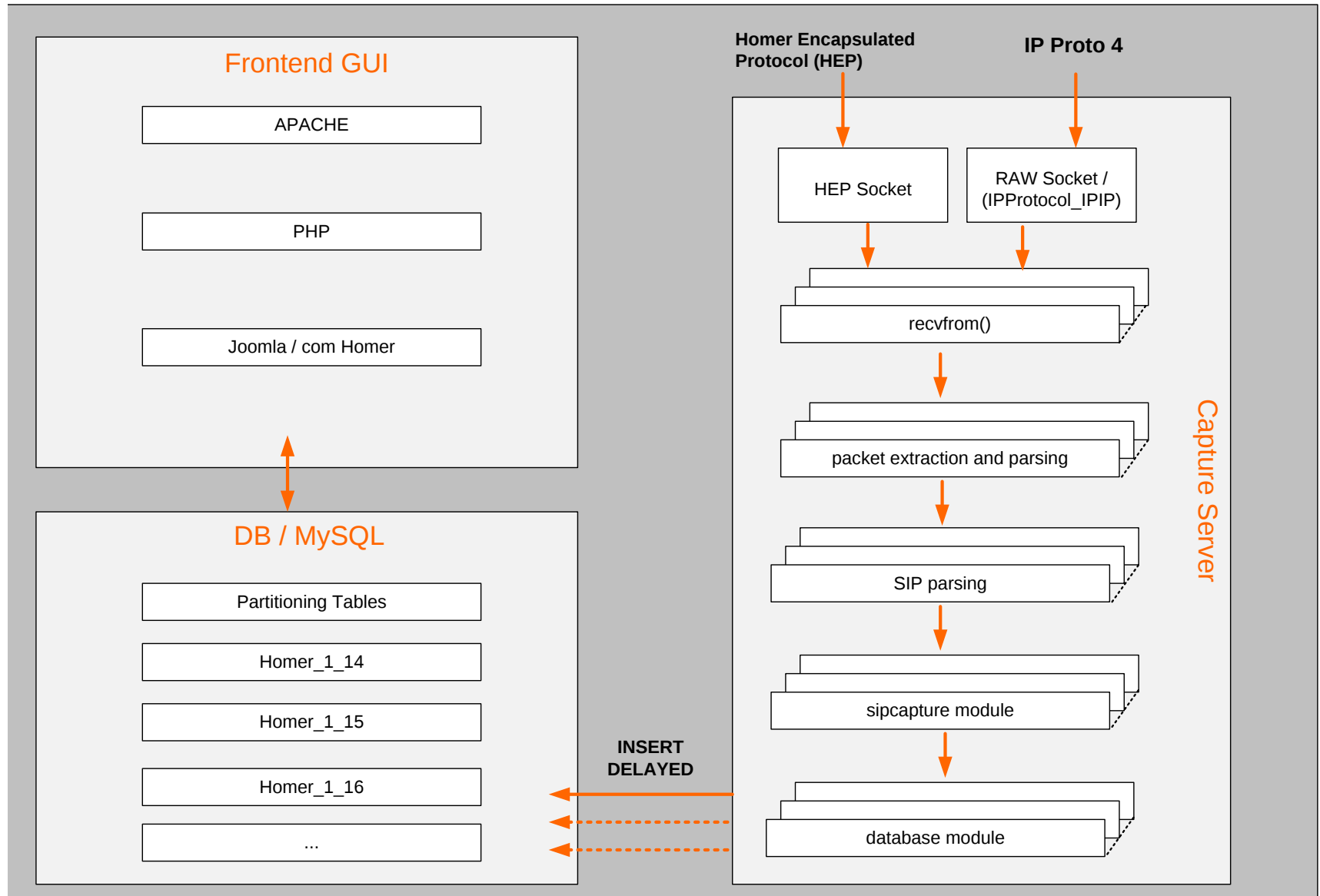
Homer Overview



HOMER



HOMER



Capturing node

The capturing node is a UNIX based server (in our case Ubuntu).

The core component of the node is the capturing application server which

- receives IP Proto 4 (IPIP) packets
- receives HEP packets
- validates if they are SIP
- parses the packets and
- inserts the values to DB

Our capture application is based on SIP-Router aka SER 3.x or kamailio 3.x, because of good core performance and effective SIP parser

Capturing node

Why a SIP-Router (SER)?

- core of SER has a very good performance
- SIP parser is effective
- has support for MySQL, PostgreSQL, Oracle
- can be compiled on many different UNIX like systems
- big community
- Open Source

Capturing node

- raw socket mode for IP/IP encapsulation
- UDP socket for HEP
- parsing the elements of the SIP packet
- inserted into a DB through SIP capture and database modules.
- In our case we use MySQL and INSERT DELAYED, which causes no socket IO-wait between SER and DB (insert and forget)

Capturing database

Usually you can use any relational DB (MySQL, PostgreSQL, Oracle,...) but if you want to build a really big capturing cluster we recommend to use key-value DB (Cassandra, MongoDB etc).

In case of key-value DB (Cassandra) all DB nodes will have the same capturing data which guarantee high availability

Frontend

The Homer GUI is based on Joomla CMS which is also Open Source. Joomla has an internal user management and a good php API.

Our frontend provides the following operational capabilities:

- Search on many different parameters (A-number, B-number, Date, Time, Call-ID, From Tag, To Tag, Method Type, User Agent, Source IP, Destination IP, Port, Protocol Type etc.)
- combining search options
- get detailed information by selecting a single message
- display information with Call Flow sequence diagram
- for a quick overview calls are grouped in different colors
- convert and save trace output as pcap file

GUI simple search form

Homer Search Form - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

http://homer.qsc.de/index.php/component/homer/?task=search

HOMER 2.0
...because sip capturing make sense

Search | Advanced Search | Help | Account

Home > Search

Standard Details

RURI User (B-Number)	
To User (B-Number)	02115424991
From User (A-Number)	02115424991
PID User (A-Number)	
Logic OR in search	☒
Call-ID	

Time / Date Parameters

Location	☒ Dusseldorf ☐ Acme
Date	Today [21-06-2011] v
From Time	13:15:51
To Time	13:50:51
Maximum records	100
Uniq packets	☐

Copyright © 2011 Homer 2.0. QSC AG. All Rights Reserved.

GUI advanced search form

HOMER 2.0
...because sip capturing make sense

Search | Advanced Search | Help | Account

search...

Home > Advanced Search

User Details

RURI User (B-Number)	
To User (B-Number)	02115424991
From User (A-Number)	02115424991
PID User (A-Number)	
Contact User	
Auth User	
Logic OR in search	☒

Time / Date Parameters

Location	☒ Dusseldorf ☐ Acme
Date	Today [21-06-2011]
From Time	Today [21-06-2011]
To Time	Yesterday [20-06-2011]
	Sunday [19-06-2011]
	Saturday [18-06-2011]
	Friday [17-06-2011]
	Thursday [16-06-2011]
	Wednesday [15-06-2011]
Maximum records	
Uniq packets	☐

Call Details

Call-ID	
B2B Call-ID	☐
From Tag	
To Tag	
Via Branch	
Method / Reply	
Reply reason	

Header Details

RURI	
VIA 1	
Diversion	
Cseq	
Reason	
Content-Type	

Network Details

Source IP	
Source port	0
Destination IP	
Destination port	0
Contact IP	
Contact port	0
Originator IP	
Originator port	0
Proto	UDP

Search Clear

GUI search result

Home > Search

▲ 13086563526576 - 13086564232976 = 706400 μ

Result: 21-06-2011 13:15:51 - 21-06-2011 13:50:51

	ID	time	μ	From User	To User	PID	Method	From ip	To ip	Callid	n
☐	512889	13:20:03	203834861	02115424991	02115424991		REGISTER	vproxy1.dus:39138	sipproxy03:5060	SBC2999968522@10_0_0_200	1
☐	512890	13:20:03	203834968	02115424991	02115424991		401 Unauthorized	sipproxy03:5060	vproxy1.dus:39138	SBC2999968522@10_0_0_200	1
☐	512935	13:20:03	203919189	02115424991	02115424991		REGISTER	vproxy1.dus:39138	sipproxy03:5060	SBC2999968522@10_0_0_200	1
☐	512937	13:20:03	203921012	02115424991	02115424991		200 OK	sipproxy03:5060	vproxy1.dus:39138	SBC2999968522@10_0_0_200	1
☐	762656	13:29:55	795300879	02115424991	02115424991		REGISTER	vproxy1.dus:39138	sipproxy03:5060	SBC2999968522@10_0_0_200	1
☐	762654	13:29:55	795300975	02115424991	02115424991		401 Unauthorized	sipproxy03:5060	vproxy1.dus:39138	SBC2999968522@10_0_0_200	1
☐	762699	13:29:55	795391233	02115424991	02115424991		REGISTER	vproxy1.dus:39138	sipproxy03:5060	SBC2999968522@10_0_0_200	1
☐	762700	13:29:55	795394760	02115424991	02115424991		200 OK	sipproxy03:5060	vproxy1.dus:39138	SBC2999968522@10_0_0_200	1
☒	1014857	13:39:12	352657607	02216698366	02115424991	02216698366	INVITE	softx-nord:5063	sipproxy03:5060	7yllhlmuu55y5g7yymgumroh8yl6ymr@SoftX3000	1
☐	1014858	13:39:12	352661349	02216698366	02115424991		100 trying -- your call is important to us	sipproxy03:5060	softx-nord:5063	7yllhlmuu55y5g7yymgumroh8yl6ymr@SoftX3000	1
☐	1014859	13:39:12	352661386	02216698366	02115424991	02216698366	INVITE	sipproxy03:5060	vproxy1.dus:39138	7yllhlmuu55y5g7yymgumroh8yl6ymr@SoftX3000	1
☐	1014860	13:39:12	352664891	02216698366	02115424991		100 Trying	vproxy1.dus:39138	sipproxy03:5060	7yllhlmuu55y5g7yymgumroh8yl6ymr@SoftX3000	1
☐	1015192	13:39:13	353467950	02216698366	02115424991		180 Ringing	vproxy1.dus:39138	sipproxy03:5060	7yllhlmuu55y5g7yymgumroh8yl6ymr@SoftX3000	1
☐	1015193	13:39:13	353468070	02216698366	02115424991		180 Ringing	sipproxy03:5060	softx-nord:5063	7yllhlmuu55y5g7yymgumroh8yl6ymr@SoftX3000	1
☐	1020525	13:39:24	364793285	02216698366	02115424991		200 OK	vproxy1.dus:39138	sipproxy03:5060	7yllhlmuu55y5g7yymgumroh8yl6ymr@SoftX3000	1
☐	1020524	13:39:24	364793302	02216698366	02115424991		200 OK	sipproxy03:5060	softx-nord:5063	7yllhlmuu55y5g7yymgumroh8yl6ymr@SoftX3000	1
☐	1020615	13:39:25	365017649	02216698366	02115424991		ACK	softx-nord:5063	sipproxy03:5060	7yllhlmuu55y5g7yymgumroh8yl6ymr@SoftX3000	1
☐	1020616	13:39:25	365017770	02216698366	02115424991		ACK	sipproxy03:5060	vproxy1.dus:39138	7yllhlmuu55y5g7yymgumroh8yl6ymr@SoftX3000	1
☐	1030719	13:39:46	386780641	02115424991	02115424991		REGISTER	vproxy1.dus:39138	sipproxy03:5060	SBC2999968522@10_0_0_200	1
☐	1030720	13:39:46	386780745	02115424991	02115424991		401 Unauthorized	sipproxy03:5060	vproxy1.dus:39138	SBC2999968522@10_0_0_200	1
☐	1030749	13:39:46	386875131	02115424991	02115424991		REGISTER	vproxy1.dus:39138	sipproxy03:5060	SBC2999968522@10_0_0_200	1
☐	1030757	13:39:46	386878263	02115424991	02115424991		200 OK	sipproxy03:5060	vproxy1.dus:39138	SBC2999968522@10_0_0_200	1
☐	1046364	13:40:23	423262775	02115424991	02216698366		BYE	vproxy1.dus:39138	sipproxy03:5060	7yllhlmuu55y5g7yymgumroh8yl6ymr@SoftX3000	1
☐	1046365	13:40:23	423262959	02115424991	02216698366		BYE	sipproxy03:5060	softx-nord:5060	7yllhlmuu55y5g7yymgumroh8yl6ymr@SoftX3000	1
☐	1046396	13:40:23	423297671	02115424991	02216698366		200 OK	softx-nord:5060	sipproxy03:5060	7yllhlmuu55y5g7yymgumroh8yl6ymr@SoftX3000	1
☒	1046395	13:40:23	423297682	02115424991	02216698366		200 OK	sipproxy03:5060	vproxy1.dus:39138	7yllhlmuu55y5g7yymgumroh8yl6ymr@SoftX3000	1

GUI SIP message details

...because sip capturing

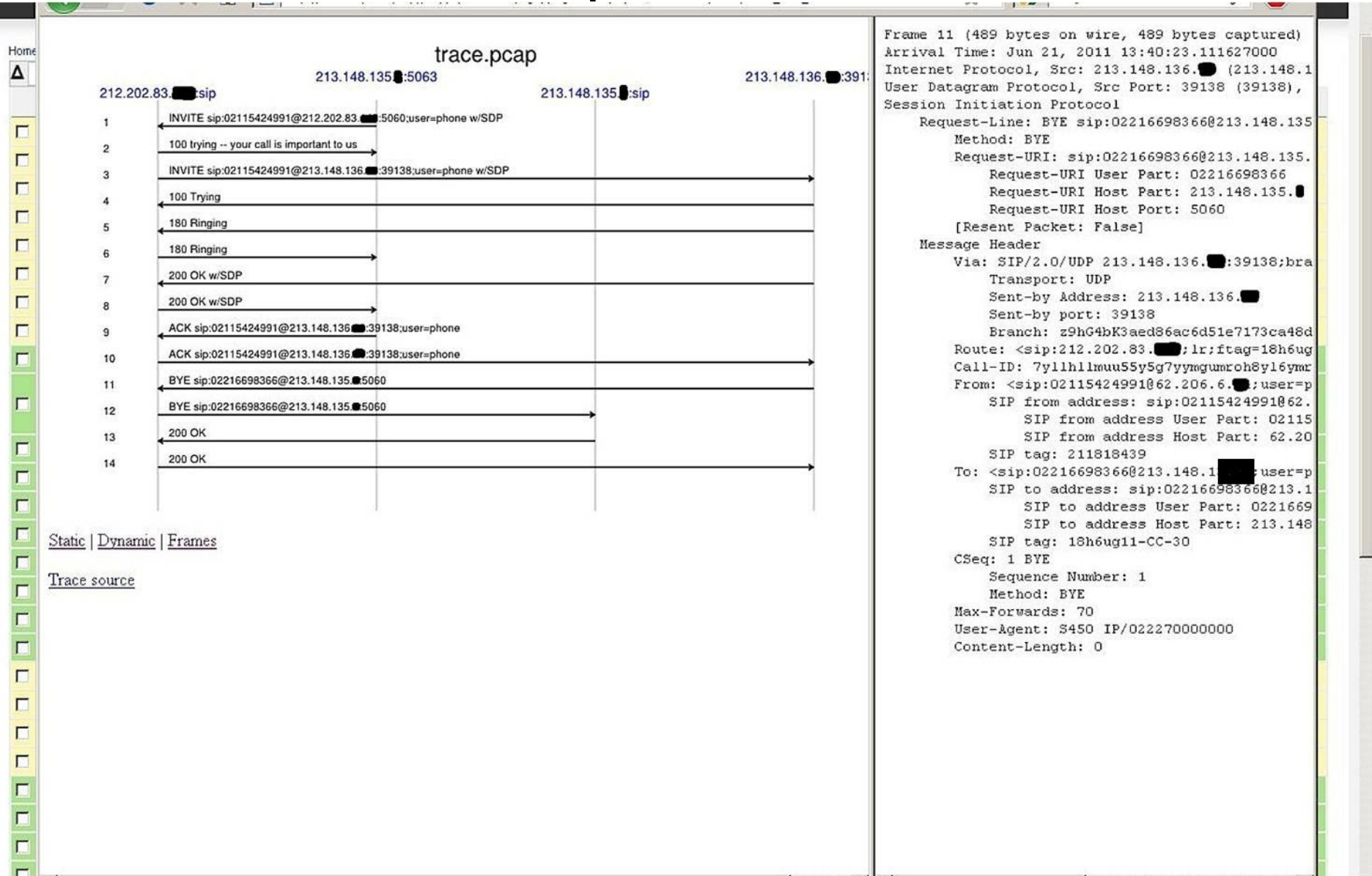
A

	ID	tin
	512889	13:20:13
	512890	13:20:13
	512935	13:20:13
	512937	13:20:13
	762656	13:29:13
	762654	13:29:13
	762699	13:29:13
	762700	13:29:13
	1014857	13:39:13
	1014858	13:39:13
	1014859	13:39:13
	1014860	13:39:13
	1015192	13:39:13
	1015193	13:39:13
	1020525	13:39:13
	1020524	13:39:13
	1020615	13:39:13
	1020616	13:39:13
	1030719	13:39:13
	1030720	13:39:13
	1030749	13:39:13
	1030757	13:39:13
	1046364	13:40:13
	1046365	13:40:13

id	1014857
date	2011-06-21 13:39:12
micro_ts	1308656352657607
method	INVITE
ruri	sip:02115424991@212.202.83.1:5060;user=phone
ruri_user	02115424991
from_user	02216698366
from_tag	18h6ug11-CC-30
to_user	02115424991
pid_user	02216698366
contact_user	02216698366
callid	7yllhlmluu55y5g7yyngumroh8yl6ymr@SoftX3000
via_1	SIP/2.0/UDP 213.148.135.1:5063;branch=z9hG4bKrycg758rogros1sh1517tu1s8
via_1_branch	z9hG4bKrycg758rogros1sh1517tu1s8
cseq	1 INVITE
content-type	application/sdp
user_agent	Huawei SoftX3000 V300R010
source_ip	213.148.135.1
source_port	5063
destination_ip	212.202.83.1
destination_port	5060
contact_ip	213.148.135.1
contact_port	5060
originator_port	0
proto	1
type	1
INVITE	sip:02115424991@212.202.83.1:5060;user=phone SIP/2.0 Via: SIP/2.0/UDP 213.148.135.1:5063;branch=z9hG4bKrycg758rogros1sh1517tu1s8 Call-ID: 7yllhlmluu55y5g7yyngumroh8yl6ymr@SoftX3000 From: <sip:02216698366@213.148.135.1;user=phone>;tag=18h6ug11-CC-30 To: <sip:02115424991@62.206.64.1;user=phone> CSeq: 1 INVITE Max-Forwards: 48 P-Asserted-Identity: <sip:02216698366@213.148.135.1;user=phone> Contact: <sip:02216698366@213.148.135.1:5060> Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,REGISTER,INFO,PRACK,SUBSCRIBE,NOTIFY,UPDATE,MESSAGE,REFER User-Agent: Huawei SoftX3000 V300R010 Content-Length: 243 msg Content-Type: application/sdp u=0

[illegible]

GUI sip call flow



Capturing capability

- Our experience has shown that DB can easily handle up to 10 m packets per hour (depending on hardware)
- Currently we receive 5-6 m packets per hour (on two nodes)
- In case of expansion the system can be clustered just by adding new nodes to the system.

CPU Dual Core Xenon 5520, 8 G RAM – 3 m packets/hour:

- 8% CPU - MySQL
- 0.2% CPU kamailio in capture mode

load average: 0.25, 0.18, 0.12

What Homer is now...

- IPv4 and IPv6 support
- Scalability
- Good performance
- Capture agent integrated in FreeSWITCH, Kamailio
- Can easily be used in any SIP networks

...and Homer in the future...

- support for XMPP protocol
- Casandra database module
- integration in other SIP Projects
- more powerful web interface
- timestamp in HEP protocol (version 2)
-

Thank you

URL: <http://homer.googlecode.com/>

E-mail/IM: alexandr.dubovikov@gmail.com