Homer-Shooting

The secret Art of Troubleshooting VoIP in Real-Time with Homer & SIPGrep

http://www.sipcapture.org

Alexandr Dubovikov

Founder and Lead Developer of HOMER SIPCAPTURE,
and Senior Voice Expert at QSC AG, Germany

Contact: Alexandr.Dubovikov@gmail.com

Presentation written by Alexandr Dubovikov
& Lorenzo Mangani

For more information: http://www.sipcapture.org

KAMAILIO WORLD
CONFERENCE & EXHIBITION

Presentation Schedule:

- WHAT IS HOMER?

Brief introduction to HOMER & SIPCAPTURE *(for all those who've been living in a pineapple under the sea, ay)*

- HOMER PROJECT:

Project Updates & Roadmap
What's coming in HOMER 3.6 and beyond

- INTRODUCING: SIPGREP 2

Swiss-Army-Knife of SIP troubleshooting gets a rewrite and becomes better and smarter

- Q & A

Capture & Homer related questions with the authors *(if time allows)*

WHAT IS HOMER? (½)

HOMER is a Kamailio based SIP Capture system and Monitoring Application with HEP3/EEP, IPIP encapsulation & port mirroring providing a simple UI and API to search, analyze and troubleshoot complex SIP signaling sessions.

The project has been developed and maintained over the last 4 years by the **SIPCapture** Team led by **Alexandr Dubovikov** and **Lorenzo Mangani** and features several thousand worldwide deployments and users ranging from small *Voice Labs* up to *Tier-1 Network Carriers and ITSPs* with billions of minutes and massive amounts of signaling over very complex networks.

The main elements in an HOMER *EcoSystem*:

*** Capture Server(s):**

- Receive, Store HEP/EEP/IPIP traffic and parse it to database
- Provide Search & Statistical functionality

*** Capture Agent(s):**

- Duplicate SIP traffic to centralized Capture Server from monitored system

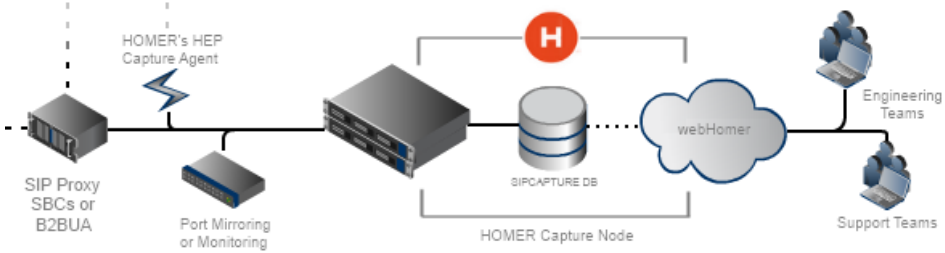
For more information, setup guides, FAQs and full details about the HOMER project please visit http://www.sipcapture.org

WHAT IS HOMER? (2/2)

HOMER is based on **SIPCAPTURE** module for **Kamailio**, can integrate with all existing Kamailio features and modules to gain additional functionality and provides support for all generations of the **HEP/EEP** encapsulation protocol.

Users can freely deploy a single Capture Node and as many Capture Agents as required to cover their voice architecture.

HEP/EEP *(Extensible Encapsulation Protocol)* support and integration is native in platforms such as *Kamailio, OpenSIPS, FreeSWITCH, Asterisk* and can be universally deployed on 3rd party systems thanks to our cross-platform and open-source HEP3 Capture Agent project (***CaptAgent4***)



WHAT'S UP WITH HOMER?

H3.5

The current release (3.5) already provides some advanced features and a fully-programmable capture plan using the best of Kamailio's resources to maximize the flexibility and the range of options provided to the end user for endless possibilities:

MODULAR CAPTURE SCRIPTING:

* Capture plan in 3.5 moves from static to completely dynamic
* Introduction of capture table field to separate traffic in db to support complex capture logic

ALARMS AND TRIGGERS:

* Mapping of events and detections to Alarms and Notifications in UI and via API Calls

GRANULAR STATISTICS CONTROL:

* Statistics are user-definable and completely customizable to meet operational or business requirement

RTP-STATS SUPPORT:

* RTP-Stats support extended to support X-Siemens media QoS reports
* X-RTP-Stat header support in BYE/200 OK contributed to BareSIP / LibRE project for automated media QoS probing

WHAT'S NEXT WITH HOMER?

H3.6

The forthcoming HOMER release (3.6-dev) will introduce some new exciting features:

RTP/RTCP SUPPORT + CORRELATION:

* Agent support RTCP duplication in HEP3/EEP *(available in CaptAgent 4 and Asterisk 12)*
* WebHomer 3.6 support for RTCP Reports parsing and time statistics display

CDRs & LOGs CAPTURE + CORRELATION:

* CDRs & Logs can be pushed/retrieved from supported PBX/SoftSwitches and parsed in HOMER
* Call Signaling and complex Session integrated correlation based on CDR details
* Advanced Fraud Detection and Alarm Triggers in Cross-Pattern
* HEPipe Project started to allow users to encapsulate and send arbitrary data/logs in HEP3

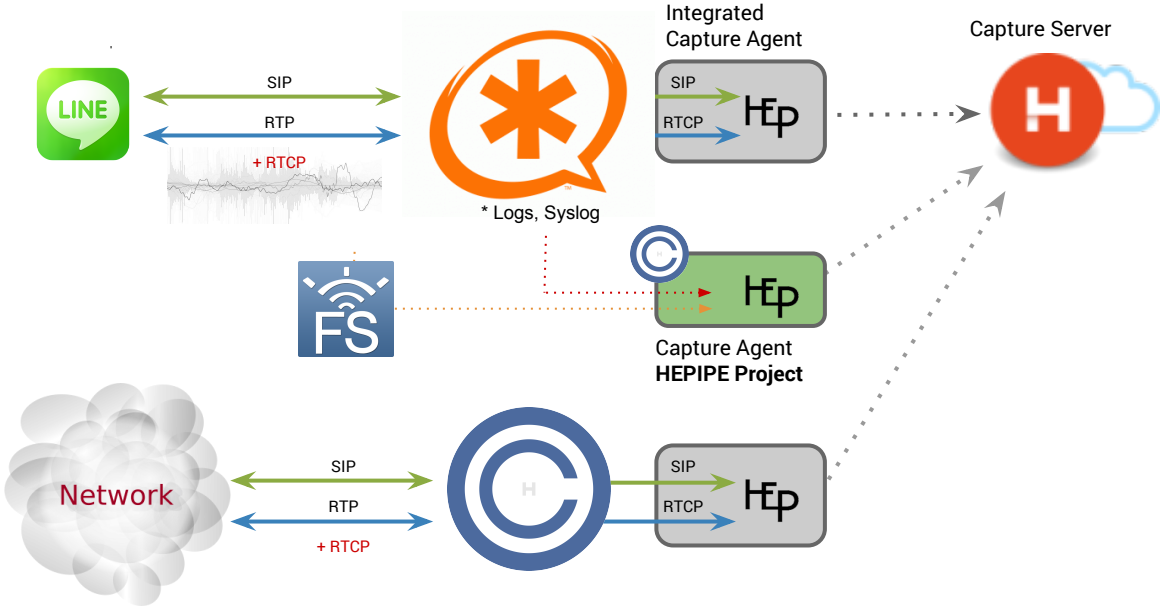
HEP3/EEP INTEGRATION:

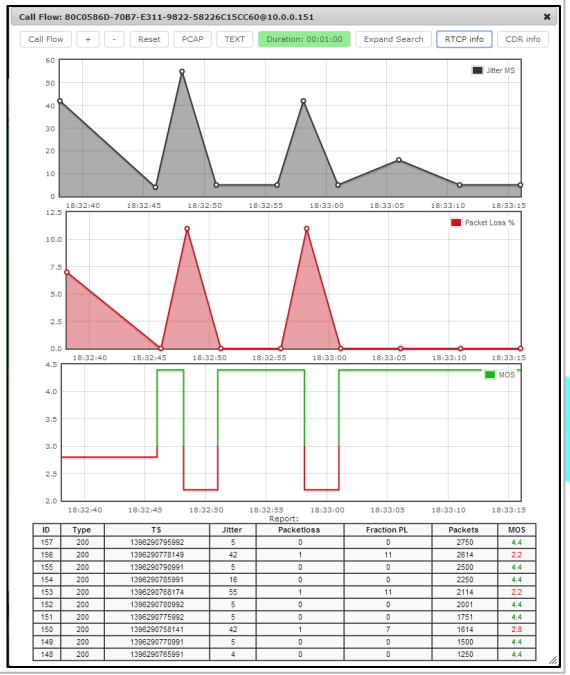
* HEP3/EEP and improved SIP/RTP support nTop's nProbe *(developed in exclusive partnership with nTop.org)*

RTCP QoS & HOMER

H3.6

The forthcoming HOMER release (3.6-dev) supports handling of RTCP packets and can determine Media QoS

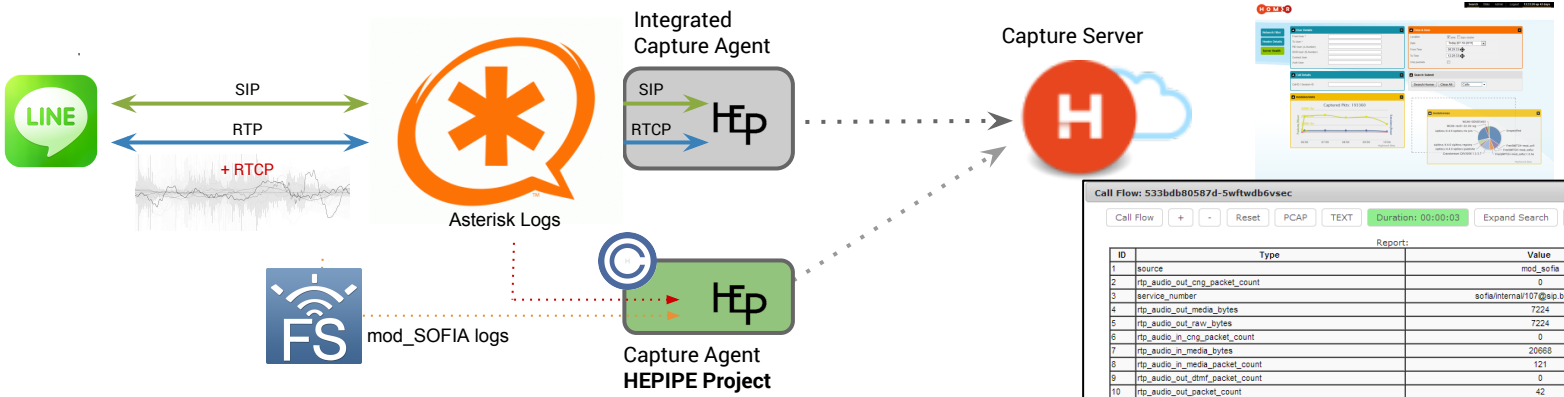


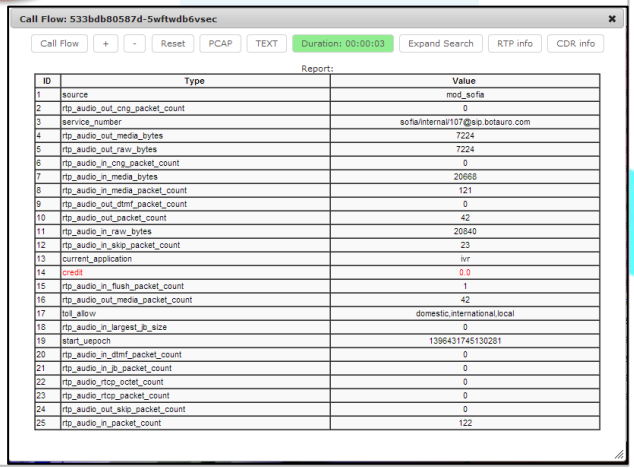


VOICE LOGS & HOMER

H3.6

HOMER (3.6-dev) supports handling of Voice LOGS via **HEPIPE** Project (available at https://github.com/sipcapture/hepipe)





ID	Type	Value
1	source	mod_sofia
2	rtp_audio_out_cng_packet_count	0
3	service_number	sofia/internal/107@sip.botauro.com
4	rtp_audio_out_media_bytes	7224
5	rtp_audio_out_raw_bytes	7224
6	rtp_audio_in_cng_packet_count	0
7	rtp_audio_in_media_bytes	20668
8	rtp_audio_in_media_packet_count	121
9	rtp_audio_out_dtmf_packet_count	0
10	rtp_audio_out_packet_count	42
11	rtp_audio_in_raw_bytes	20840
12	rtp_audio_in_skip_packet_count	23
13	current_application	ivr
14	credit	0.0
15	rtp_audio_in_flush_packet_count	1
16	rtp_audio_out_media_packet_count	42
17	toll_allow	domestic,international,local
18	rtp_audio_in_largest_jb_size	0
19	start_uepoch	1396431745130281
20	rtp_audio_in_dtmf_packet_count	0
21	rtp_audio_in_jb_packet_count	0
22	rtp_audio_rtcp_octet_count	0
23	rtp_audio_rtcp_packet_count	0
24	rtp_audio_out_skip_packet_count	0
25	rtp_audio_in_packet_count	122

```
echo '1396362930;1003;fd8f48ea-b9aa-11e3-92f7-1803731b65be;127.0.0.1;5060;10.0.0.1;5060;
{"pl": 10, "jt": 10}' | ./hepipe  -s hepserver -p 9061
```

INTRODUCING: SIPGREP$_2$ (½)

WHAT IS SIPGREP

Sipgrep is a powerful pcap-aware tool command line tool to *sniff, capture, display and troubleshoot* SIP signaling over IP networks, with filter logic common to other packet sniffing tools *(ie: tcpdump, ngrep)* and allowing the end user to specify extended regular expressions matching against SIP headers and dialogs.

HISTORY OF SIPGREP

SIPGREP has ~10 years of production usage under its belt - without major changes!

The first version of SIPGREP was created in *2005* by *Alexandr Dubovikov* as an *NGREP wrapper* specialized to SIP traffic filtering display. The tool was intended to provide instant access to SIP troubleshooting for “live” terminal use and quickly became a standard feature in specialized distributions and for Telephony products such as *SER, Kamailio and FreeSWITCH*.

INTRODUCING: SIPGREP2

(2/2)

SIPGREP2 is a complete rewrite which picks up where the original left, adding many new *KEY* features:

- Native *C* code application
- Advanced Regex filtering (PCRE) for each Header *(no longer limited to From/To/RURI)*
- SIP Statistics w/ quality reports
- Colorized output for SIP methods, Tags, Call-ID
- Dialog detection
- More output formats *(PCAP, Plain ASCII Text, Colorized ASCII Text)*
- Redirection of captured packets to Homer's SIPCapture Nodes *(HEPv3)*
- PCAP file rotation and auto exit based on filesize, duration conditions
- SIP ASCII diagram *(in development)*
- Native support for LINUX AND Solaris, Free/Open/NetBSD, OSX
- Defragmentation support
- Friendly-Scanner kill/crash application *(packet-of-death)* to stop scan/floods
- Naturally Open-Source (GPLv3)

The source code of the new sipgrep can be found here: **http://github.com/adubovikov/sipgrep**

EXAMPLES OF SIPGREP-FU (½)

Find any session where caller contains "*2123421*"

sipgrep -f 2123421

Find a call with caller contains "*2123421*" and callee contains "*3432*"

sipgrep -f 2123421 -t 3432

Find only UPDATE or REFER methods with no dialog match

sipgrep '^(UPDATE|REFER)' -m

Find all 5xx and 603 replies with no dialog match

sipgrep '^SIP 2.0 (5[1-9][1-9]|603)' -m

U 2014/03/25 21:48:12.002227 178.172.154.251:5682 -> 109.69.65.77:5060

SIP/2.0 **200** OK.
Via: SIP/2.0/UDP 109.69.65.77;rport=5060;branch=**z9hG4bKt08U46DU2c6tK**.
From: <sip:mod_sofia@109.69.65.77:5060>;tag=**SKtQDmcvyUUvm**.
To: <sip:143@82.165.138.203>;tag=**081D72F3635B4518**.
Call-ID: **c784e95e-b45e-11e3-8099-f92f0e501a9e_AABCCB0DD@169.254.1.1.**
CSeq: 57488247 OPTIONS.
Contact: <sip:143@178.172.154.251:5682;
uniq=ACC02CC189541D09D5C6A62A47888>.
User-Agent: AVM FRITZ!Box Fon 06.04.33 (May 10 2007).
Supported: 100rel,replaces,timer.
Allow-Events: telephone-event,refer.
Allow: INVITE,ACK,OPTIONS,CANCEL,BYE,UPDATE,PRACK,INFO,SUBSCRIBE,NOTIFY.
Accept: application/sdp, multipart/mixed.
Accept-Encoding: identity.
Content-Length: 0.

EXAMPLES OF SIPGREP-FU (2/2)

Kill-Crash SIPVicious scanners with custom UAS

sipgrep -j sipvicious

Display & Mirror matching traffic to HEP Capture Server (*ie: HOMER*)

sipgrep -f 112233 -H udp:10.0.10.20:9061

Display & Capture all traffic for 120 seconds only and exit/report:

sipgrep -g -G -q 'duration:120'

Save all matching dialogs to PCAP and split in files smaller than 20kb

sipgrep -q 'filesize:20' -O sipgrep.pcap

U 2014/03/25 21:48:12.002227 178.172.154.251:5682 -> 109.69.65.77:5060

SIP/2.0 **200** OK.
Via: SIP/2.0/UDP 109.69.65.77;rport=5060;branch=**z9hG4bKt08U46DU2c6tK**.
From: <sip:mod_sofia@109.69.65.77:5060>;tag=**SKtQDmcvyUUvm**.
To: <sip:143@82.165.138.203>;tag=**081D72F3635B4518**.
Call-ID: **c784e95e-b45e-11e3-8099-f92f0e501a9e_AABCCB0DD@169.254.1.1.**
CSeq: 57488247 OPTIONS.
Contact: <sip:143@178.172.154.251:5682;
uniq=ACC02CC189541D09D5C6A62A47888>.
User-Agent: AVM FRITZ!Box Fon 06.04.33 (May 10 2007).
Supported: 100rel,replaces,timer.
Allow-Events: telephone-event,refer.
Allow: INVITE,ACK,OPTIONS,CANCEL,BYE,UPDATE,PRACK,INFO,SUBSCRIBE,NOTIFY.
Accept: application/sdp, multipart/mixed.
Accept-Encoding: identity.
Content-Length: 0.

SIPGREP REPORTS:

```
------------------------------------------------
Dialog finished: [53342c3b200e-hgf9cyc7r0i2]
Type: Call
From: "From Work with Love" <sip:107@sip.xxx.com>;tag=fucueumi19
To: <sip:101@sip.xxx.com;user=phone>
UAC: snom360/8.7.3.25
CDR init ts: 1395928127
CDR ringing ts: 1395928128
SRD(PDD): 1 sec
CDR answer ts: 1395928136
WTA: 9 sec
CDT (duration): 70 sec
CDR termination ts: 1395928206
Was connected: YES
REASON: BYE
------------------------------------------------
```

KAMAILIO WORLD
CONFERENCE & EXHIBITION

http://www.sipcapture.org

HOMER