

sngrep

Sngrep

Что такое sngrep?

sngrep - это терминальный инструмент, который группирует сообщения SIP (Session Initiation Protocol) по Call-Id и отображает их в виде потоков стрелок, аналогичных тем, что используются в RFC SIP.

Цель этого инструмента - облегчить процесс изучения или отладки SIP.

Функции:

- Захват SIP-пакетов с устройств или чтение из PCAP-файла.
- Поддержка UDP, TCP и TLS (частично).
- Позволяет фильтровать с помощью BPF (Berkeley Packet Filter)
- Сохранение захваченных пакетов в PCAP файл

Установка

Сборка из исходников

Скачайте [последний релиз](#) (или клонируйте GIT-репозиторий)

На большинстве систем команды для сборки будут стандартными для atotools:

```
./bootstrap.sh
./configure
make
make install (as root)
```

Процесс configure проверит наличие необходимых зависимостей:

- libncurses5 - для пользовательского интерфейса, окон, панелей.
- libpcap - для захвата пакетов с устройств и чтения их из PCAP файлов.
- libssl - (опционально) для транспорта TLS
- libncursesw5 - (необязательно) для пользовательского интерфейса, окон, панелей (поддержка широких символов).

Вы можете передать следующие флаги в `./configure` для включения некоторых функций

флаг конфигурации	Функция
<code>--with-openssl</code>	Добавляет поддержку OpenSSL для разбора перехваченных сообщений TLS (требуется libssl).
<code>--with-gnutls</code>	Добавляет поддержку GnuTLS для разбора перехваченных сообщений TLS (требуется gnutls).
<code>--with-pcre</code>	Добавляет поддержку Perl-совместимых регулярных выражений в полях <code>regexr</code>
<code>--enable-unicode</code>	Добавляет поддержку Ncurses UTF-8/Unicode (требуется libncursesw5)
<code>--enable-ipv6</code>	Включает поддержку захвата пакетов IPv6.
<code>--enable-eep</code>	Включает поддержку отправки/получения пакетов EEP.

Вы можете найти [\[подробные инструкции для некоторых дистрибутивов\]](#).

Бинарные файлы

Пользователи OSX могут установить `sngrep` с помощью [homebrew](#).

```
brew install sngrep
```

Установка двоичных пакетов

Debian / Ubuntu

If you're using a recent version of Debian/Ubuntu, you can find `sngrep` in the official Debian/Ubuntu repositories. (thanks to [@linuxmaniac](#))

Otheriwse, you can use Irontec repositories for some of Debian and Ubuntu releases.

Binaries are built only for amd64 and i386 architectures right now with all supported features enabled.

Debian

Add Irontec repositories entry in your `/etc/apt/sources.list`

Use your distrubution source line (**only one of these**)

```
deb http://packages.irontec.com/debian squeeze main
deb http://packages.irontec.com/debian wheezy main
deb http://packages.irontec.com/debian jessie main
deb http://packages.irontec.com/debian stretch main
```

```
deb http://packages.irontec.com/debian buster main
deb http://packages.irontec.com/debian bullseye main
```

Ubuntu

Add Irontec repositories entry in your */etc/apt/sources.list*

Use your distribution source line (**only one of these**)

```
deb http://packages.irontec.com/ubuntu trusty main
deb http://packages.irontec.com/ubuntu precise main
deb http://packages.irontec.com/ubuntu vivid main
deb http://packages.irontec.com/ubuntu xenial main
deb http://packages.irontec.com/ubuntu bionic main
deb http://packages.irontec.com/ubuntu focal main
deb http://packages.irontec.com/ubuntu jammy main
```

Install Repository key

```
wget http://packages.irontec.com/public.key -q -O - | apt-key add -
```

Install the package

```
apt-get update
apt-get install sngrep
```

Fedora / CentOS / RHEL Linux

sngrep is available from the [community build server](#)

Enable the repository

```
dnf copr enable irontec/sngrep
```

or

```
yum copr enable irontec/sngrep
```

Install sngrep package

```
dnf install sngrep
```

or

```
yum install sngrep
```

Alpine Linux

sngrep is available in community repositories starting from Alpine v3.3 (Thx Francesco Colista!)

Decomment community repository from /etc/apk/repositories (if commented)

Update your package list

```
apk update
```

Install sngrep

```
apk add sngrep
```

Gentoo

You can find an unofficial ebuilds for sngrep at [Gentoo Bugtracker System](#) (Thanks to spacedream)

Feel free to vote if you would like to see sngrep be part of Gentoo portage tree.

Arch

You can find an unofficial PKGBUILD for Arch at [ArchLinux User Repositories](#) (thanks to w1ngnutt)

Feel free to vote if you would like to see sngrep at official Arch repositories.

OSX

OSX users can install sngrep using [homebrew](#)

```
brew install sngrep
```

OpenWRT/LEDE

You can use official repositories for installing sngrep using:

```
opkg install sngrep
```

Как использовать

Аргументы командной строки

Есть несколько аргументов, которые можно использовать из командной строки, чтобы изменить поведение sngrep по умолчанию

```
sngrep [-hVcivNqrD] [-IO pcap_dump] [-d dev] [-l limit] [-k keyfile] [-LH capture_url] [<match expression>] [<bpf filter>]
```

- `-h --help`: Данное использование
- `-V --version`: Информация о версии
- `-d --device`: Использовать это устройство захвата вместо устройства по умолчанию

- `-I --input`: Считывание захваченных данных из pcap-файла
- `-O --output`: Запись захваченных данных в файл pcap
- `-c --calls`: Отображать только диалоги, начинающиеся с INVITE
- `-r --rtp`: Захват полезной нагрузки RTP-пакетов
- `-l --limit`: Установите ограничение захвата до N диалогов
- `-i --icase`: Сделать <выражение> нечувствительным к регистру
- `-v --invert`: Инвертировать <выражение>
- `-N --no-interface`: Не отображать интерфейс sngrep, только захват
- `-q --quiet`: Не выводить диалоги захвата в режиме отсутствия интерфейса
- `-D --dump-config`: Печать активных настроек конфигурации и выход
- `-f --config`: Чтение конфигурации из файла
- `-R --rotate`: Ротация вызовов при достижении предела захвата.
- `-H --eep-send`: URL захвата Homer (udp:X.X.X.X:XXXX)
- `-L --eep-listen`: Прослушивание инкапсулированных пакетов (udp:X.X.X.X:XXXX)
- `-k --keyfile`: Файл закрытого ключа RSA для расшифровки перехваченных пакетов

Например, перехват всех SIP-пакетов со всех устройств, имеющих порт источника или назначения 5060.

```
sngrep port 5060
```

Или отображение SIP-пакетов с устройства eth0, имеющего в качестве источника или назначения 192.168.0.50 через порт 5061, сохранение их в /tmp/sip_capture.pcap

```
sngrep -d eth0 -O /tmp/sip_capture.pcap host 192.168.0.50 port 5061
```

Or displaying all SIP packets for a given host in sip_capture.pcap PCAP file

```
sngrep -I /tmp/sip_capture.pcap host 10.10.1.50
```

Linux users may add capture permissions to sngrep to avoid run it as root

```
setcap 'CAP_NET_RAW+eip' /usr/local/bin/sngrep
```

if the above does not work, try this:

```
setcap 'CAP_NET_RAW+eip' /usr/bin/sngrep
```

Интерфейс

Имеется несколько окон для предоставления различной информации:

- `[[Call List Window|CallList]]`: Allows to select the calls to be displayed

- **[[Call Flow Window|CallFlow]]**: Shows a diagram of source and destiny of messages
- **[[Call Raw Window|CallRaw]]**: Display SIP messages texts (useful for copy messages to clipboard)
- **[[Message Diff Window|MessageDiff]]**: Displays differences between two SIP messages

[[Here|Screenshots]] are see some screens of sngrep windows.

Общие сочетания клавиш

Most of the program windows have a help dialog with a brief description and useful keybindings. There are some keybindings that can be use anywhere in the program:

- **F1 or h**: Show current window help and keybindings.
- **ESC or q**: Go back to the previous window
- **F8 or C**: Toggle Message syntax highlight

Call List window

The first window that sngrep shows is Call List window and display the different SIP Call-Ids found in messages. The displayed columns depends on your terminal width and your custom configuration.

Current Mode: Offline

Display Filter:

sngrep - SIP messages flow viewer

Filename: /root/sip_capture.pcap

SIP From	SIP To	Msgs	Source	Destiny	Starting	Trans
[] dect810.10.9.40:5061	dect810.10.9.40:5061	4	10.10.0.152:32797	10.10.9.40:5061	REGISTER	TCP
[] asterisk810.10.9.40	dect810.10.0.152:32797	2	10.10.9.40:5061	10.10.0.152:32797	NOTIFY	TCP
[] asterisk810.10.9.40	dect810.10.0.152:32797	2	10.10.9.40:5061	10.10.0.152:32797	NOTIFY	TCP
[] spakaian810.10.9.40	spakaian810.10.9.40	4	10.10.1.142:5061	10.10.9.40:5060	REGISTER	UDP
[] asterisk810.10.9.40	spakaian810.10.1.142:5061	2	10.10.9.40:5060	10.10.1.142:5061	NOTIFY	UDP
[] asterisk810.10.9.40	spakaian810.10.1.142:5061	2	10.10.9.40:5060	10.10.1.142:5061	NOTIFY	UDP
[] dect810.10.9.40:5061	3007810.10.9.40:5061	10	10.10.0.152:32797	10.10.9.40:5061	INVITE	TCP
[] 3003810.10.9.40	spakaian810.10.1.142:5061	7	10.10.9.40:5060	10.10.1.142:5061	INVITE	UDP

Quit

Show

Select

Help

Save

Search

Extended

Clear

Raw

Filter

Colours on/off

You can move between dialogs with *arrow keys* and selected them using *Spacebar*. Selecting multiple dialogs will display all them in Call flow window and Call Raw window, and will allow to save only the selected message dialogs to a PCAP file.

Keybindings:

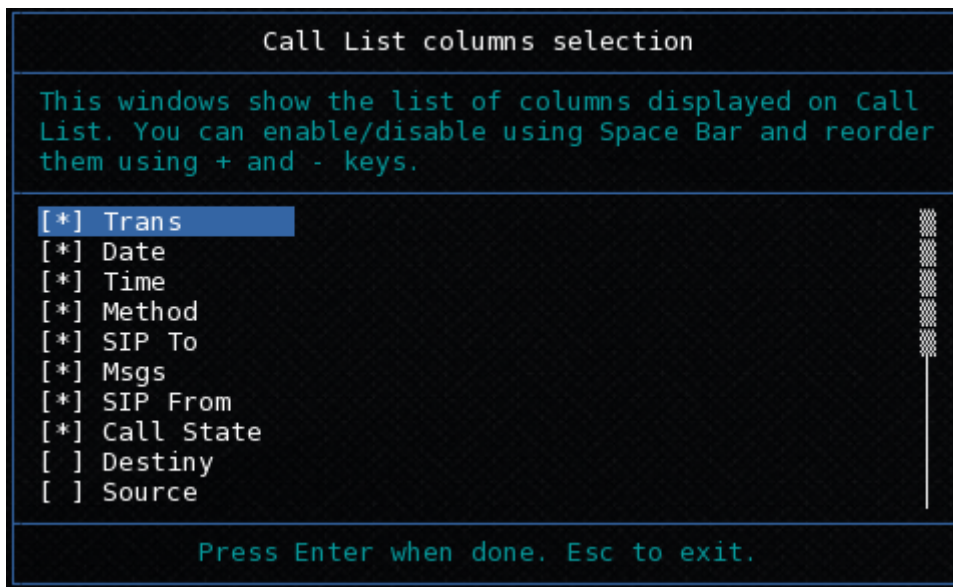
- **Arrow keys**: Move through the list
- **Enter**: Display current or selected dialog(s) message flow
- **A**: Auto scroll to new calls

- **F2 or s**: Save selected/all dialog(s) to a PCAP file
- **F3 or / or TAB**: Enter a display filter. This filter will be applied to the text lines in the list
- **F4 or x**: Display current selected dialog and its related one.
- **F5**: Clear call list
- **F6 or r**: Display selected dialog(s) messages in raw text
- **F7 or f**: Show advanced filters dialogs
- **F9 or l**: Turn on/off address resolution if enabled
- **F10 or t**: Select displayed columns
- **< or >**: Choose sort direction and which column to use for sorting
- **Z**: Swap sort direction
- **p**: Pause

You can do a simple matching filter pressing TAB or / . If you need more specific filter options, use the filtering screen:

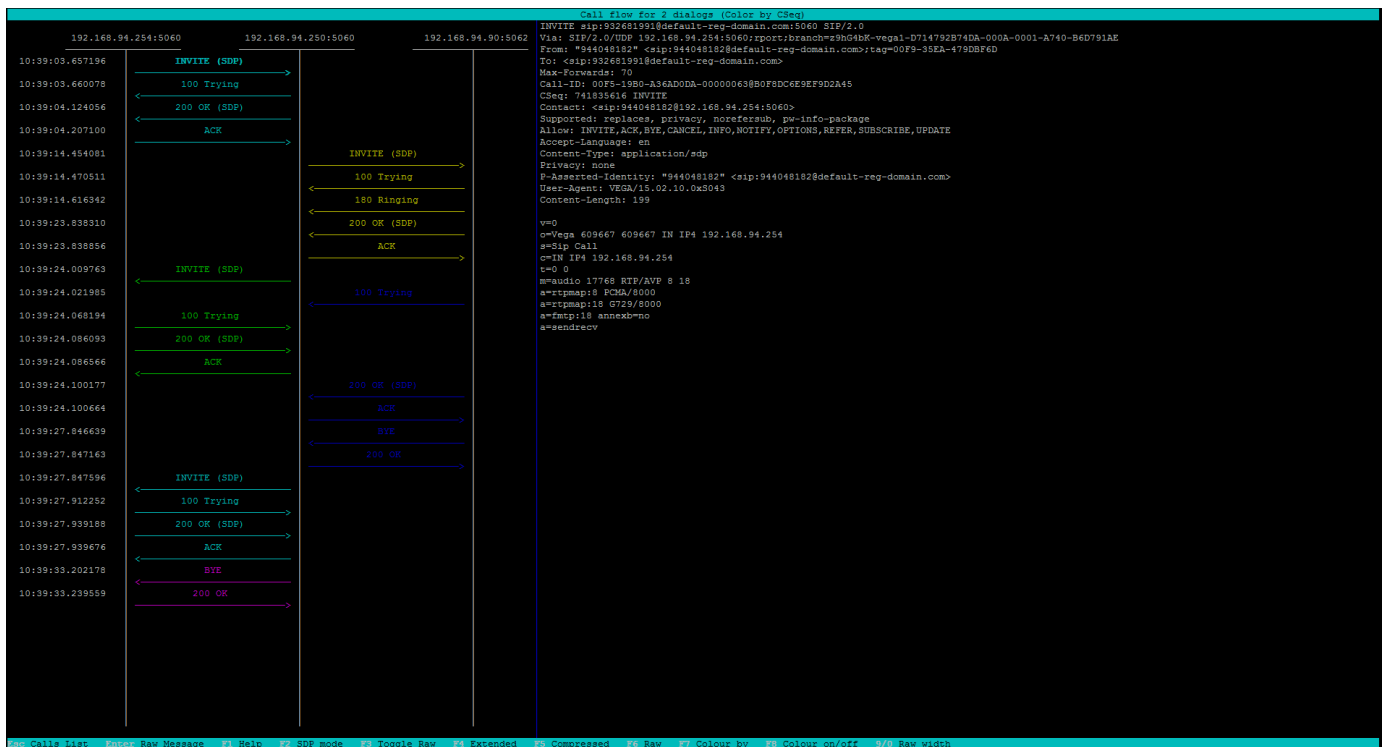
Filter options			
SIP From:			
SIP To:			
Source:			
Destination:			
Payload:			
REGISTER	[*]	OPTIONS	[*]
INVITE	[*]	PUBLISH	[*]
SUBSCRIBE	[*]	MESSAGE	[*]
NOTIFY	[*]		
[Filter]		[Cancel]	

You can also change the displayed columns, setting them on configuration file, or during execution using the column selector:



Call Flow window

This window displays a flow diagram of the selected dialogs' messages.



The selected message payload will be displayed in the right side of the window.

You can move between messages using *arrow keys* and select them using *Spacebar*. Selecting multiple messages will display the Message Diff Window.

Keybindings:

- **Arrow keys:** Move through messages
- **Enter:** Display current message raw (so you can copy payload)
- **F2 or d:** Toggle SDP info instead of Method/ResponseCode in arrows

- **F3 or t**: Toggle message preview side panel
- **F4 or x**: Show current dialog and its extended one
- **F5 or s**: Show one column per address
- **F6 or R**: Show raw messages of dialogs
- **F7 or c**: Change flow colormode
- **F9 or l**: Turn on/off address resolution if enabled
- **9 and 0**: Increase/Decrease preview side panel
- **T**: Restore preview side panel size
- **D**: Only show messages that has SDP content

There are several color modes to display the arrows:

- **By Method/Response**: Red for Method, Green for Responses
- **By Call-Id**: Each Call-Id one color, useful when displaying multiple calls flows
- **By CSeq**: Each CSeq one color

Call Raw window

This window will display the selected dialog messages in plain text. It was designed to allow copying the messages payload easily.

```

s=audio 16386 RTP/AVP 8
a=rtpmap:8 PCMA/8000
a=rtpmap:20
a=sendrecv

2014/05/29 10:39:04.207100 192.168.94.254:5060 -> 192.168.94.250:5060
ACK sip:9326819318192.168.94.250:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.94.254:5060;rport;branch=s9HG4bK07Fc9e1b
From: "9440481828192" <sip:9440481828192@default-reg-domain.com>;tag=00F9-55EA-473D076D
To: <sip:
      8default-reg-domain.com>;tag=as73da8950
Max-Forward: 70
Call-ID: 00F9-19B0-A36AD0DA-000000638B0FDC6E3EF9D2A45
CSeq: 741935616 ACK
Contact: <sip:9440481828192.168.94.254:5060>
User-Agent: Yealink/15.02.10.0x8043
Content-Length: 0

2014/05/29 10:39:14.454081 192.168.94.250:5060 -> 192.168.94.90:5062
INVITE sip:1102 238192.168.94.90:5062 SIP/2.0
Via: SIP/2.0/UDP 192.168.94.250:5060;branch=s9HG4bK07Fc9e1b
Max-Forward: 70
From: "Flat_recption" <sip:09440481828192.168.94.250>;tag=as7cad6555
To: <sip:1102
      238192.168.94.90:5062>
Contact: <sip:09440481828192.168.94.250:5060>
Call-ID: 9446d36a67b422a17f90d3c3bae7255c8192.168.94.250:5060
CSeq: 102 INVITE
User-Agent: "Irontec IVOX"
Date: Thu, 29 May 2014 08:39:14 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH
Supported: replaces, timer
X-CID: 00F9-19B0-A36AD0DA-000000638B0FDC6E3EF9D2A45
P-Asserted-Identity: "Flat_recption" <sip:09440481828192.168.94.250>
Content-Type: application/sdp
Content-Length: 210

v=0
o=root 1014197597 1014197597 IN IP4 192.168.94.250
s=Asterisk PBX 1.8.15.1 (RSP CS branch 1.8.15.1)
c=IN IP4 192.168.94.250
t=0 0
m=audio 16386 RTP/AVP 8
a=rtpmap:8 PCMA/8000
a=rtpmap:20
a=sendrecv

2014/05/29 10:39:14.470511 192.168.94.90:5062 -> 192.168.94.250:5060
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.94.250:5060;branch=s9HG4bK07Fc9e1b
From: "Flat_recption" <sip:09440481828192.168.94.250>;tag=as7cad6555
To: <sip:11
      238192.168.94.90:5062>
Call-ID: 9446d36a67b422a17f90d3c3bae7255c8192.168.94.250:5060
CSeq: 102 INVITE
User-Agent: Yealink SIP-T22P 7.70.0.150
Content-Length: 0

2014/05/29 10:39:14.616342 192.168.94.90:5062 -> 192.168.94.250:5060
SIP/2.0 100 Ringing
Via: SIP/2.0/UDP 192.168.94.250:5060;branch=s9HG4bK07Fc9e1b
From: "Flat_recption" <sip:09440481828192.168.94.250>;tag=as7cad6555
To: <sip:11
      238192.168.94.90:5062>;tag=122616ee7f
Call-ID: 9446d36a67b422a17f90d3c3bae7255c8192.168.94.250:5060

```

(http://irontec.github.io/sngrep/images/call_raw.png)

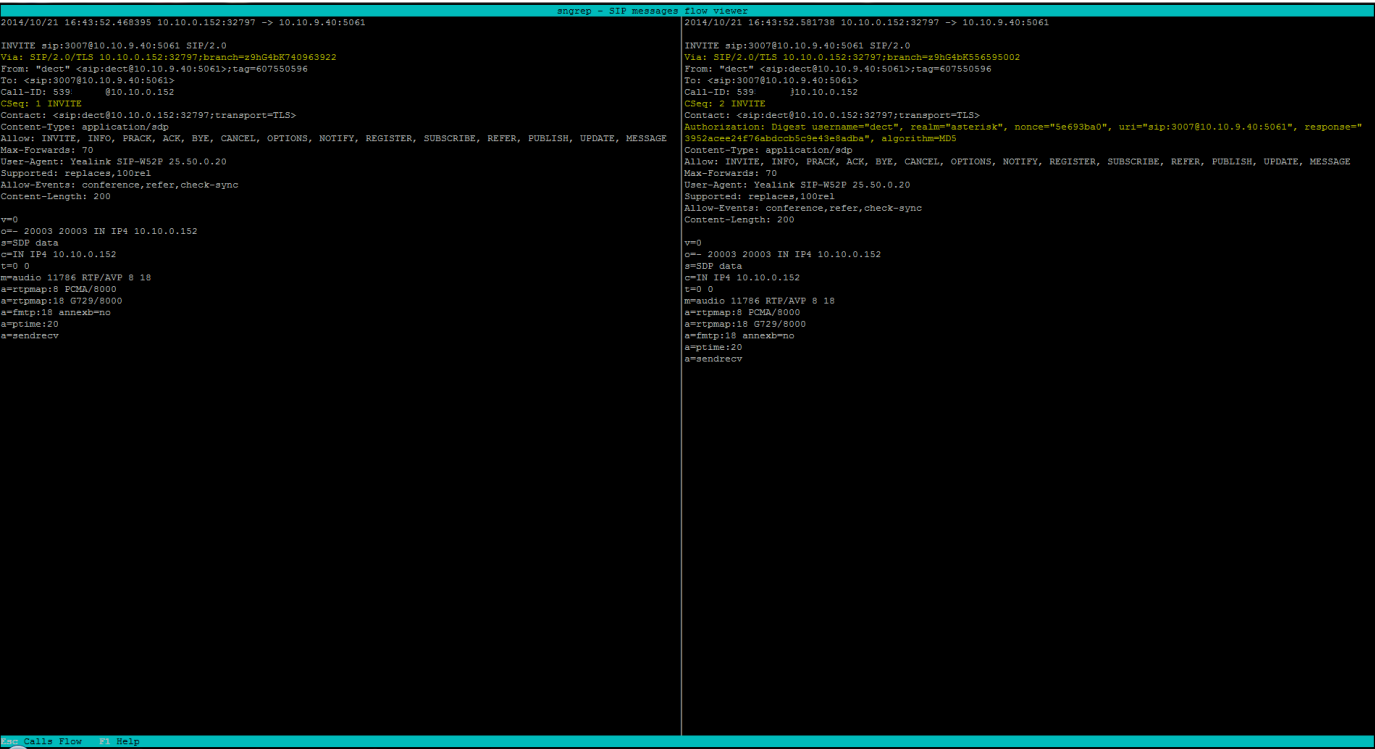
Keybindings:

- **Arrow keys**: Move through the window
- **s**: Save displayed text to file

Message diff window

This window will compare two messages. Right now the comparison is done searching each line in the other message, highlighting those not found exactly.

You can reach this window by selecting two messages using *Spacebar* in [\[\[Call Flow window|CallFlow\]\]](#)



Configuration

sngrep configuration is done using sngrepc file. This file contains one line directives that can change default sngrep behaviour. Configuration files are readed in this order

- System-wide configuration: Usually `/etc/sngrepc` or `/usr/local/etc/sngrepc`
- User configuration: `$HOME/.sngrepc`

Comments

For any of this configuration files, empty lines or lines starting with # will be totally ignored. Inline comments (at the end of a configuration setting) are not supported.

Options

Options are configured using `set` directive to modify its default value. This are the available options configurable via `set` directive:

Format: `set <option> <value>`

option	format	default	description
background	black transparent	black	Changes background printing.

option	format	default	description
syntax	on off	on	Enable/Disable SIP Payload syntax highlighting.
syntax.tag	on off	off	Enable/Disable tag syntax highlighting.
syntax.branch	on off	off	Enable/Disable branch syntax highlighting.
hintkeyalt	on off	off	Display alternative keybinding hint in bottom bar.
capture.limit	int > 0	20000	Set max number of captured dialogs (-l argument).
capture.lookup	on off	off	Enable/Disable DNS resolution of captured packets IP addresses.
capture.device	any <interface>	any	Set default capture interface (-d argument).
capture.outfile	<filename>		Set default capture dump file (-O argument).
capture.keyfile	<filename>		Default capture keyfile for TLS transport (-k argument).
capture.rtp	on off	off	Store captured RTP packets allowing to save them later. (-r argument).
capture.eep	on off	off	Enable/Disable capture of HEP/EEP traffic.
sip.ignoreiccomplete	on off	on	Ignore dialogs not starting with some Request Methods.
sip.calls	on off	off	Ignore dialogs not starting with INVITE Method.
sngrep.savepath	<path>	\$HOME	Default path in save dialog.
sngrep.displayhost	on off	off	Show resolved hostnames instead of IPs (requires capture.lookup).
cl.noexitprompt	on off	off	Disable exit confirmation prompt.
cl.scrollstep	int	10	Change default scrolling steps in Call List.
cl.colorattr	on off	on	Display color in attributes in Call List.
cl.autoscroll	on off	on	Scroll Call List automatically when new rows appear.
cl.sortfield	fieldname	index	Call List sort field (see below a list of field names).
cl.sortorder	asc desc	asc	Call List sort order.
cf.forceraw	on off	on	Display Payload preview in Call Flow.
cf.rawminwidth	int	40	Minimum number of columns Payload preview will use.
cf.splitcallid	on off	off	One Column = One address in Call Flow.

option	format	default	description
cf.highlight	bold reverse	bold	Change current message arrow highlight mode.
cf.scrollstep	int	4	Change default scrolling steps in Call List.
cr.scrollstep	int	10	Change default scrolling steps in Call Raw.
cr.nonascii	string	.	Character to print non-ascii characters in SIP payload.
cl.autoscroll	on off	off	Enable/disable autoscroll.
filter.methods	all methods	method(s)	Default value for checkboxes in filter screen.
filter.payload	string		Default value for payload display filter.
aliasport	on off	off	Take port into account when using aliases.
displayalias	on off	off	Enable/Disable use of aliases.

Alias

Alias can be handy to replace addresses with a label in flow columns. This was designed to improve the understanding of the message source and destination in flows. You can toggle between addresses and alias with *togglealias* (defaults to `a`, see keybindings below)

Format: `alias <address> <text>`

Also, addresses with the same alias will be displayed in one column in Call flow *compress* mode (default `s`, see keybindings below)

If `aliasport` setting set to `on` then format may be the following:

`alias <address>:<port> <text>`

Call List Columns

Column configuration is also done using `set` directive. You can easily configure your columns during runtime and save displayed layout or configure them manually.

`set cl.column<index> <attribute>` (For example: `set cl.column7 time`)

You can also change default display width using:

`set cl.column<index>.width <value>` (For example: `set cl.column3.width 100`)

Here's a list of Call attributes:

name	width	description
index	4	Dialog capture index for unique identification of dialog.

name	width	description
sipfrom	30	From header sip uri.
sipfromuser	20	Username in From header.
sipto	30	To header sip uri.
sipouser	20	Username in To header.
src	22	Source IP:Port of packet.
srchost	16	Source IP of packet.
dst	22	Destination IP:Port of packet.
dsthost	16	Destination IP of packet.
callid	50	Call-id SIP header value.
xcallid	50	X-Call-id SIP header value.
date	10	Date in YYYY/MM/DD format.
time	8	Time in HH:MM:SS format.
method	15	Request Method or Response code of SIP message.
transport	3	SIP transport (UDP TCP TLS ..)
msgcnt	5	Number of messages in the dialog.
state	19	Call State (if dialog is a call)
convdur	7	Conversation duration (since first 200 OK to BYE)
totaldur	8	Total call duration (since INVITE to last message)
reason	25	SIP Reason header text
warning	4	SIP Warning header code

Keybindings

All sngrep keybindings can be configured using `bind` and `unbind` directives. Each screens handles a couple of actions, which can have multiple key binded. You can remove default keybindings and remap the same key to other actions.

```
bind <action> <keycode>
```

```
unbind <action> <keycode>
```

Keycode can be:

- A lowercase letter
- An Uppercase letter
- A letter with `^` or `Ctrl-` preffix

- One special keycode: `Space`, `Esc`, `Enter`

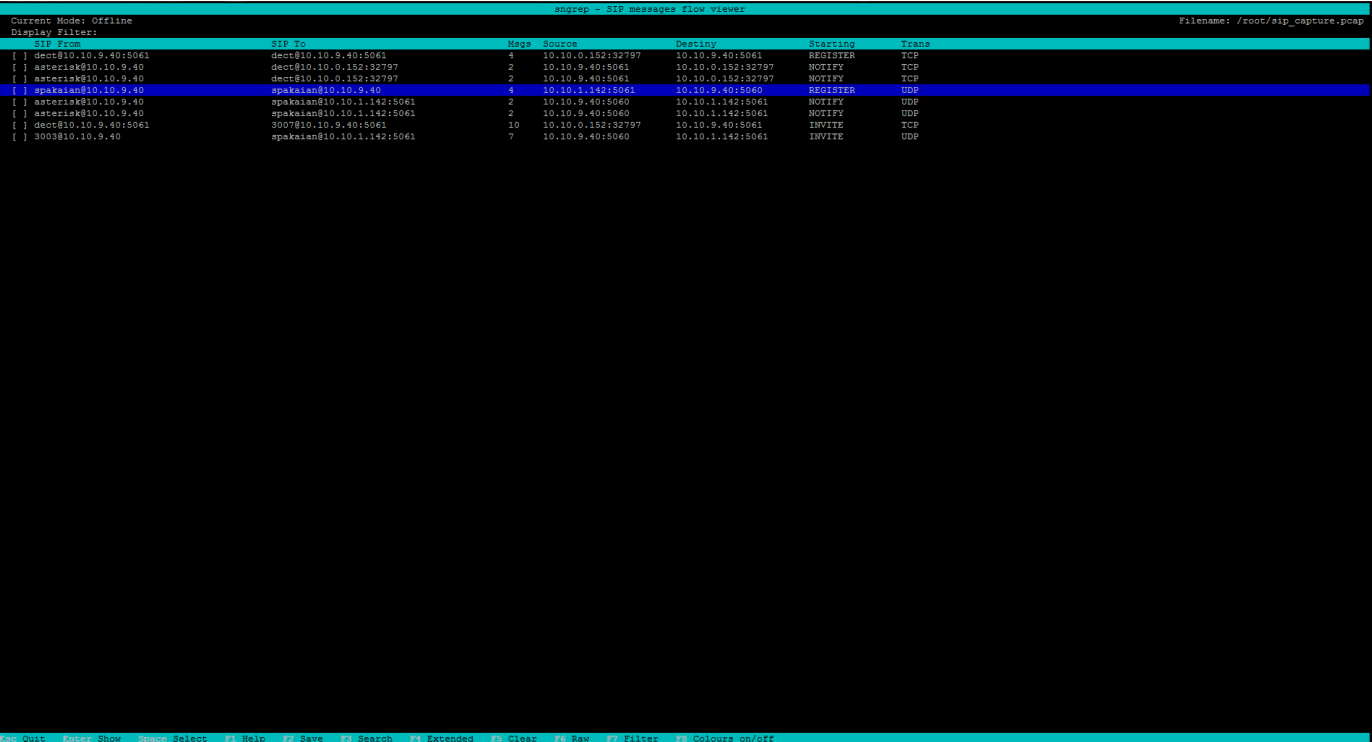
Действие может быть одним из следующих:

Действие	привязка по умолчанию	описание
up	Up,j	Прокрутить вверх
down	Down,k	Прокрутить вниз
left	Left	Переместиться влево
right	Right	Переместиться вправо
delete	Delete	Удалить один символ
backspace	BackSpace	Удалить один символ
npage	NextPage,Ctrl-F	Следующая страница
ppage	PrevPage,Ctrl-B	Предыдущая страница
hnpage	Ctrl-D	Half next page
hppage	Ctrl-U	Half previous page
begin	Home,Ctrl-A	Переместиться в начало поля
end	End,Ctrl-E	Переместиться в конец поля
pfield	Tab	Move to previous field
nfield	Tab	Move to next field
clear	Ctrl-U	Clear current field
clearcalls	F5	Clear call list
togglesyntax	F8,C	Toggle Payload syntax
colormode	F7,c	Change arrows color mode
togglehostname	F9	Toggle displaying hostnames
togglealias	a	Toggle displaying addresses alias (see <code>address</code> directive)
pause	p	Pause online capture
prevscreen	Esc,q,Q	Go to previous screen
help	F1,h,H,?	Show help popup for current screen
raw	F6,r,R	Show call raw screen
flow	Enter	Show call flow screen
flowex	F4,x,X	Show call flow extended screen
filters	F7,f,F	Show filters popup
columns	F10,t,T	Show columns popup

Действие	привязка по умолчанию	описание
columnup	-	Move column up in the column list
columndown	+	Move column down in the column list
search	F3,/,Tab	Focus Display filter box
save	F2,s,S	Show save dialog
select	Space	Select current dialog/message
rtp	f	Show current rtp packet flow
rawpreview	F3,t	Toggle payload preview in call flow
moreraawpreview	9	Increase payload preview size
lessrawpreview	0	Decrease payload preview size
resetrarawpreview	T	Reset payload preview size
onlysdp	D	Only show messages with sdp content
sdpinfo	F2,d	Show First SDP address in message arrows
compress	F5,s	Compress view to only display one column per IP address
hintalt	K	Show alternative keybind in bottom bar

Скриншоты

Call List Window



Call Flow Window

Call flow for 2 diallegs (Color by Seq)			
192.168.94.254:5060	192.168.94.250:5060	192.168.94.90:5062	
10:39:03.657196	INVITE (SDP)		INVITE sip:9326819918@default-reg-domain.com:5060 SIP/2.0 Via: SIP/2.0/UDP 192.168.94.254:5060;rport;branch=z9hG4bK-vegal-D714792B74DA-000A-0001-A740-BED791AE From: "944048182" <sip:944048182@default-reg-domain.com>;tag=00F9-35EA-479DBF6D To: <sip:9326819918@default-reg-domain.com> Max-Forwards: 70 Call-ID: 60F5-19B6-ASGAD0DA-000000638B0F8DC6E9EF9D2A45 CSeq: 741833416 INVITE Contact: <sip:944048182@192.168.94.254:5060> Supported: replaces, privacy, norefersub, pw-info-package Allow: INVITE,ACK,BYE,CANCEL,INFO,NOTIFY,OPTIONS,REFER,SUBSCRIBE,UPDATE Accept-Language: en Content-Type: application/sdp Privacy: none P-Asserted-Identity: "944048182" <sip:944048182@default-reg-domain.com> User-Agent: VEGA/15.02.10.0x5043 Content-Length: 139
10:39:03.660078	100 Trying		v=0 o=Vega 609667 609667 IN IP4 192.168.94.254 s=Sip Call c=IN IP4 192.168.94.254 t=0 0 m=audio 17768 RTP/AVP 8 18 a=rtpmap:8 PCMA/8000 a=rtpmap:18 G729/8000 a=fmtp:18 annexb=no a=sendrecv
10:39:04.124056	200 OK (SDP)		
10:39:04.207100	ACK		
10:39:14.454081		INVITE (SDP)	
10:39:14.470511		100 Trying	
10:39:14.616342		180 Ringing	
10:39:23.838310		200 OK (SDP)	
10:39:23.838856		ACK	
10:39:24.009763	INVITE (SDP)		
10:39:24.021985		100 Trying	
10:39:24.068194	100 Trying		
10:39:24.086093	200 OK (SDP)		
10:39:24.086566	ACK		
10:39:24.100177		200 OK (SDP)	
10:39:24.100664		ACK	
10:39:27.846639		BYE	
10:39:27.847163		200 OK	
10:39:27.847596	INVITE (SDP)		
10:39:27.912252	100 Trying		
10:39:27.939188	200 OK (SDP)		
10:39:27.939676	ACK		
10:39:33.202178	BYE		
10:39:33.239559	200 OK		

Call flow for 4 dialogs (Color by Request/Response)			
10.10.1.142:5061	10.10.9.40:5060	10.10.1.122:5065	10.10.1.245:5063
15:01:30.395894	INVITE (SDP)		INVITE sip: @10.10.1.245:5063 SIP/2.0 Via: SIP/2.0/UDP 10.10.9.40:5060;branch=z9hG4bK16be22a8 Max-Forwards: 70 From: "Kaian " <sip:3007@10.10.9.40>;tag=as4d7eb267 To: <sip: @10.10.1.245:5063> Contact: <sip:3007@10.10.9.40:5060> Call-ID: 7a3bb1e528f86ab176708ab82e7e2f55@10.10.9.40:5060 CSeq: 102 INVITE User-Agent: "Irontec IV02" Date: Wed, 07 Jan 2015 14:01:30 GMT Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH Supported: replaces, timer X-CID: e3a4754-9a10fbfb@10.10.1.142 Remote-Party-ID: "Kaian " <sip:3007@10.10.9.40>;party=calling;privacy=off;screen=no Content-Type: application/sdp Content-Length: 200 v=0 o=root 853802039 853802039 IN IP4 10.10.9.40 s=Asterisk PBX 1.8.15.1 (RSP CS branch 1.8.15.1) c=IN IP4 10.10.9.40 t=0 0 m=audio 15788 RTP/AVP 8 a=rtpmap:8 PCMA/8000 a=ptime:20 a=sendrecv
15:01:30.396222	401 Unauthorized		
15:01:30.401112	ACK		
15:01:30.405455	INVITE (SDP)		
15:01:30.405906	100 Trying		
15:01:30.735636		INVITE (SDP)	
15:01:30.741073		100 Trying	
15:01:30.755964		180 Ringing	
15:01:30.756674	180 Ringing		
15:01:32.435633	REFER		
15:01:32.435880	202 Accepted		
15:01:32.441057	NOTIFY		
15:01:32.441484	603 Declined		
15:01:32.441795		INVITE (SDP)	
15:01:32.441903		UPDATE	
15:01:32.451287	200 OK		
15:01:32.455112	ACK		
15:01:32.456695		200 OK	
15:01:32.604969		200 OK (SDP)	
15:01:32.605290		ACK	
15:01:36.441237	BYE		
15:01:36.441515	200 OK		
15:01:36.854468		BYE	
15:01:36.855773		200 OK	
15:01:36.856658		CANCEL	
15:01:36.866859		487 Request Terminated	
15:01:36.866993		ACK	
15:01:36.868700		200 OK	

Syntax on SIP messages

:5060		:5060		Call flow for 1456159481 (Color by CSeq)
18:10:33.520687	INVITE (SDP)			INVITE sip:1004@in.striker-dev.irontec.com:5061 SIP/2.0 Record-Route: <sip: ;r2=on;lr;ftag=346486145;nat=yes> Record-Route: <sip: ;5061;transport=tls;r2=on;lr;ftag=346486145;nat=yes> Via: SIP/2.0/UDP ;branch=z9hG4bKf605.36879a8bd13711fael106fc6ca290bb.0;i=12a Via: SIP/2.0/TLS ;19423;rport=19423;received= ;branch=z9hG4bK1266065429 From: "Carlos" <sip:0015654fb4751@in.striker-dev.irontec.com:5061>;tag=346486145 To: <sip:1004@in.striker-dev.irontec.com:5061> Call-ID: 1456159481e CSeq: 2 INVITE Contact: <sip: :19423;transport=TLS;alias=-19423-3> Content-Type: application/sdp Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH, UPDATE, MESSAGE Max-Forwards: 69 User-Agent: Yealink SIP-T42G 29.72.0.45 Supported: replaces Allow-Events: talk,hold,conference,refer,check-sync Content-Length: 324 X-MEDIA-IP: v=0 o=- 20032 20032 IN IP4 s=SDP data c=IN IP4 t=0 0 m=audio 60192 RTP/AVP 0 8 18 9 101 a=rtpmap:0 PCMU/8000 a=rtpmap:8 PCMA/8000 a=rtpmap:18 G729/8000 a=fmtp:18 annexb=no a=rtpmap:9 G722/8000 a=fmtp:101 0-15 a=rtpmap:101 telephone-event/8000 a=ptime:20 a=sendrecv a=ortp-proxy:yes
18:10:33.522373	100 Trying			
18:10:34.093703	180 Ringing			
18:10:35.319799	200 OK (SDP)			
18:10:35.475926	ACK			
18:10:37.763666	INVITE (SDP)			
18:10:37.764023	100 trying -- your call is			
18:10:37.960526	200 OK (SDP)			
18:10:37.961395	ACK			
18:10:37.977311	BYE			
18:10:38.087434	200 OK			

Call Raw Window

```

==audio 16398 RTP/AVP 8
a=rtptime:18 PCM/8000
a=ptime:20
a=sendrecv

2014/05/29 10:39:04.207100 192.168.94.254:5060 -> 192.168.94.250:5060
ACK wip:9362619191454081 192.168.94.250:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.94.254:5060;branch=93646467d422a17790dc9762961741835616
From: "9404048182" <sip:9404048182@default-reg-domain.com>;tag=00F9-35EA-479D8F6D
To: <sip:8dfault-reg-domain.com>;tag=as73de8950
Max-Forward: 70
Call-ID: 00F9-19B0-A36AD0DA-0000004380F8DC4E9EF9D2A45
CSeq: 741835616 ACK
Contact: <sip:9404048182@192.168.94.254:5060>
User-Agent: Yealink/15.02.10.08043
Content-Length: 0

2014/05/29 10:39:14.454081 192.168.94.250:5060 -> 192.168.94.90:5062
INVITE sip:1102 0238192.168.94.90:5062 SIP/2.0
Via: SIP/2.0/UDP 192.168.94.250:5060;branch=93646467d422a17790dc97629616
Max-Forward: 70
From: "P1at_recognition" <sip:094404048182@192.168.94.250>;tag=as7cad6555
To: <sip:1102 0238192.168.94.90:5062>
Contact: <sip:094404048182@192.168.94.250:5060>
Call-ID: 846434467b422a17f90dc933ac7280c8192.168.94.250:5060
CSeq: 102 INVITE
User-Agent: "Yealink IVOZ"
Date: Thu, 29 May 2014 08:59:14 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH
Supported: replaces, timer
X-CID: 00F9-19B0-A36AD0DA-0000006380F8DC4E9EF9D2A45
X-Asserted-Identity: "P1at_recognition" <sip:094404048182@192.168.94.250>
Content-Type: application/sdp
Content-Length: 210

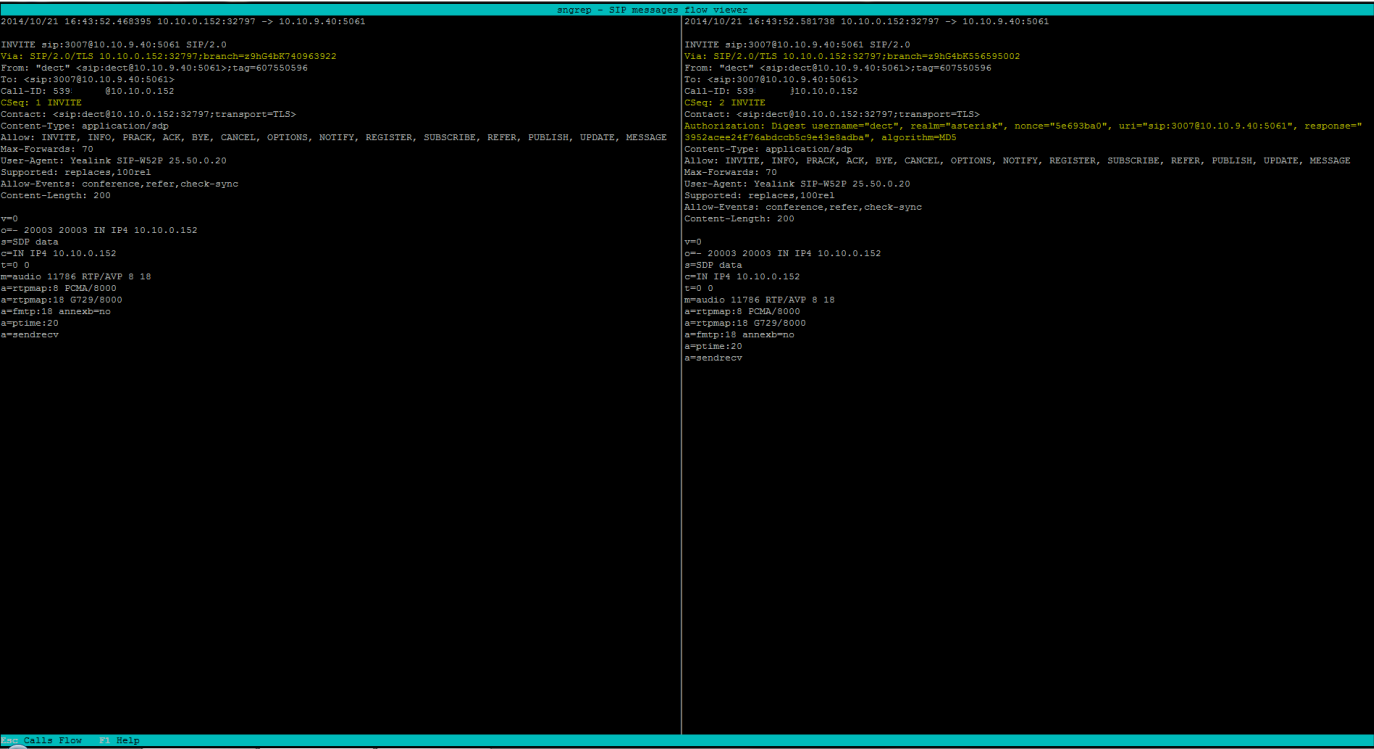
v=0
o=root 1016197597 1016197597 IN IP4 192.168.94.250
s=asterisk PBX 1.8.15.1 (RSP CS branch 1.8.15.1)
c=IN IP4 192.168.94.250
t=0 0
m=audio 16398 RTP/AVP 8
a=rtptime:18 PCM/8000
a=ptime:20
a=sendrecv

2014/05/29 10:39:14.470511 192.168.94.90:5062 -> 192.168.94.250:5060
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.168.94.250:5060;branch=93646467d422a17790dc97629616
From: "P1at_recognition" <sip:094404048182@192.168.94.250>;tag=as7cad6555
To: <sip:1102 0238192.168.94.90:5062>
Call-ID: 846434467b422a17f90dc933ac7280c8192.168.94.250:5060
CSeq: 102 INVITE
User-Agent: Yealink SIP-T22P 7.7.0.0.150
Content-Length: 0

2014/05/29 10:39:14.616342 192.168.94.90:5062 -> 192.168.94.250:5060
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.168.94.250:5060;branch=93646467d422a17790dc97629616
From: "P1at_recognition" <sip:094404048182@192.168.94.250>;tag=as7cad6555
To: <sip:1102 0238192.168.94.90:5062>;tag=1226166575
Call-ID: 846434467b422a17f90dc933ac7280c8192.168.94.250:5060
CSeq: 102 INVITE
User-Agent: Yealink SIP-T22P 7.7.0.0.150
Content-Length: 0

```

Message Diff Window



Other dialogs

Settings



Column List selection

Call List columns selection

This windows show the list of columns displayed on Call List. You can enable/disable using Space Bar and reorder them using + and - keys.

[*] Trans
[*] Date
[*] Time
[*] Method
[*] SIP To
[*] Msgs
[*] SIP From
[*] Call State
[] Destiny
[] Source

Press Enter when done. Esc to exit.

Filters dialog

Filter options

SIP From:
SIP To:
Source:
Destination:
Payload:

REGISTER [*]
INVITE [*]
SUBSCRIBE [*]
NOTIFY [*]
OPTIONS [*]
PUBLISH [*]
MESSAGE [*]

[Filter]
[Cancel]

Save dialog

Save capture

Path: /home/kaian
Filename: capture_123.pcap

Dialogs
(*) all dialogs
() selected dialogs [0]
() filtered dialogs [33]

Format
(*) .pcap (SIP)
(-) .pcap (SIP + RTP)
() .txt

[Save]
[Cancel]

Stats

Stats Information	
Dialogs: 33	COMPLETED: 4 (80.0%)
Calls: 5 (15.2%)	CANCELLED: 0 (0.0%)
Messages: 134	IN CALL: 0 (0.0%)
	REJECTED: 1 (20.0%)
	CALL SETUP: 0 (0.0%)
INVITE: 9 (6.7%)	1XX: 15 (11.2%)
REGISTER: 17 (12.7%)	2XX: 30 (22.4%)
SUBSCRIBE: 0 (0.0%)	3XX: 0 (0.0%)
UPDATE: 0 (0.0%)	4XX: 22 (16.4%)
NOTIFY: 0 (0.0%)	5XX: 0 (0.0%)
OPTIONS: 23 (17.2%)	6XX: 0 (0.0%)
PUBLISH: 0 (0.0%)	7XX: 0 (0.0%)
MESSAGE: 0 (0.0%)	8XX: 0 (0.0%)
INFO: 0 (0.0%)	
BYE: 6 (4.5%)	
CANCEL: 0 (0.0%)	
Press any key to continue	

At the time writing 1.2.0 has not been released. This will only work with compiled sngrep from master branch

This mini tutorial will allow sngrep to receive kamailio packets and can be used to debug received TLS, HEP or SIP packets. HEPv2 support in sngrep is still under testing and this compatibility may or may not work.

Часто задаваемые вопросы

Что означает sngrep?

Первые версии sngrep использовали ngrep для захвата sip-пакетов и разбора его вывода. Это изменилось в версии 0.1.0, где вместо него использовался libpcap. sngrep был разработан для использования с теми же аргументами командной строки, которые мои коллеги использовали для ngrep, просто добавив s в начале. Буква s в sngrep будет означать SIP.

Зачем нужен новый инструмент для сетевой фильтрации?

Не знаю. Я не смог найти ни одного консольного инструмента, который бы отображал потоки вызовов.

Расширенное окно потока вызовов (Call flow) не работает

Если вы хотите установить связь между различными диалогами (расширенный поток вызовов), в одном из диалогов, ссылающемся на другой, должен присутствовать заголовок. Этот заголовок может быть X-CID или X-Call-ID и должен содержать Call-ID другого связанного диалога.

Сборка

Установка зависимостей

Debian/Ubuntu

Install required packages from repository:

```
# apt-get update
# apt-get install git autoconf automake gcc make \
  libncursesw5-dev libncurses5-dev libpcap-dev libssl-dev libpcre3-dev
```

CentOS/Fedora

Install required packages from repository:

```
# yum install ncurses-devel make libpcap-devel pcre-devel \
  openssl-devel git gcc autoconf automake
```

ArchLinux

Install required packages from repository:

```
# pacman -Sy ncurses libpcap openssl git gcc sed make
```

Mac OS X

Install [MacPorts](https://www.macports.org/install.php):

- <https://www.macports.org/install.php>

Install main dependencies:

```
port install pkgconfig
port install libpcap
port install ncurses
```

Install optional dependencies:

```
port install pcre
port install openssl
```

Ncurses library on Mac OS X has wide character support (unicode) by default, there is no ncursesw library.

To enable support for PCRE and SSL/TLS: in order to find the include files and libraries installed by macports, before executing any command for compiling from sources, do:

```
export CFLAGS=$(pkg-config --cflags libpcre openssl)
export LDFLAGS=$(pkg-config --libs libpcre openssl)
```

Whenever an upgrade is performed, do the exports commands every time before running **configure**.

NetBSD

Install required packages from repository:

```
pkgin install autoconf automake
```

Configure command must be run with CFLAGS AND LDFLAGS:

```
CFLAGS="-D_NETBSD_SOURCE -D_XOPEN_SOURCE=600 -I/usr/pkg/include/ncursesw -I/usr/pkg/include" \
LDFLAGS="-L/usr/pkg/lib -lpcr -lssl -lcrypto -Wl,-R/usr/pkg/lib -lncursesw" \
./configure --with-openssl --with-gnutls --enable-unicode --with-pcre
```

Сборка из исходников

Клонируйте репозиторий github и проверьте, что все предварительные условия выполнены.

```
$ git clone https://github.com/irontec/sngrep
$ cd sngrep
$ ./bootstrap.sh
$ ./configure
$ make
# make install      # (от root)
```

Send HEP traffic from Kamailio to local sngrep

Configuring Kamailio to duplicate received packets

- Enable siptrace module in `kamailio.cfg`

```
loadmodule      "siptrace.so"

### siptrace ###
modparam("siptrace", "duplicate_uri", "sip:127.0.0.1:9061")
modparam("siptrace", "hep_mode_on", 1)
modparam("siptrace", "trace_to_database", 0)
modparam("siptrace", "trace_flag", 22)
modparam("siptrace", "trace_on", 1)
modparam("siptrace", "hep_version", 2)
```

- Mark dialogs to be sent with the configured flag

```
route {
    sip_trace();
    setflag(22);
}
```

- On Kamailio working as sipcapture collector, It should be required to also trace responses. Also, in this kind of Kamailio that doesn't work as proxy, order of messages may not be received in the same order they were originally sent.

```
onreply_route {
    sip_trace();
}
```

- Reload your kamailio to apply new configuration

Configuring sngrep to received HEP packets

Previous Kamailio configuration uses HEPv2 to send packets, which is only supported in sngrep since 1.2.0

- Enable HEPv2 en `~/ .sngrepc` file

```
set eep.listen on
set eep.listen.version 2
set eep.listen.address 127.0.0.1
set eep.listen.port 9061
```

If your capagent send CorrelationID enable this option

```
set eep.listen.uuid on
```

- Run sngrep and you'll see received packets from kamailio