FOSDEM
2021

Pocket SIP Tools

Daniel-Constantin Mierla
Co-Founder Kamailio Project
daniel@asipto.com
@miconda

KAMAILIO

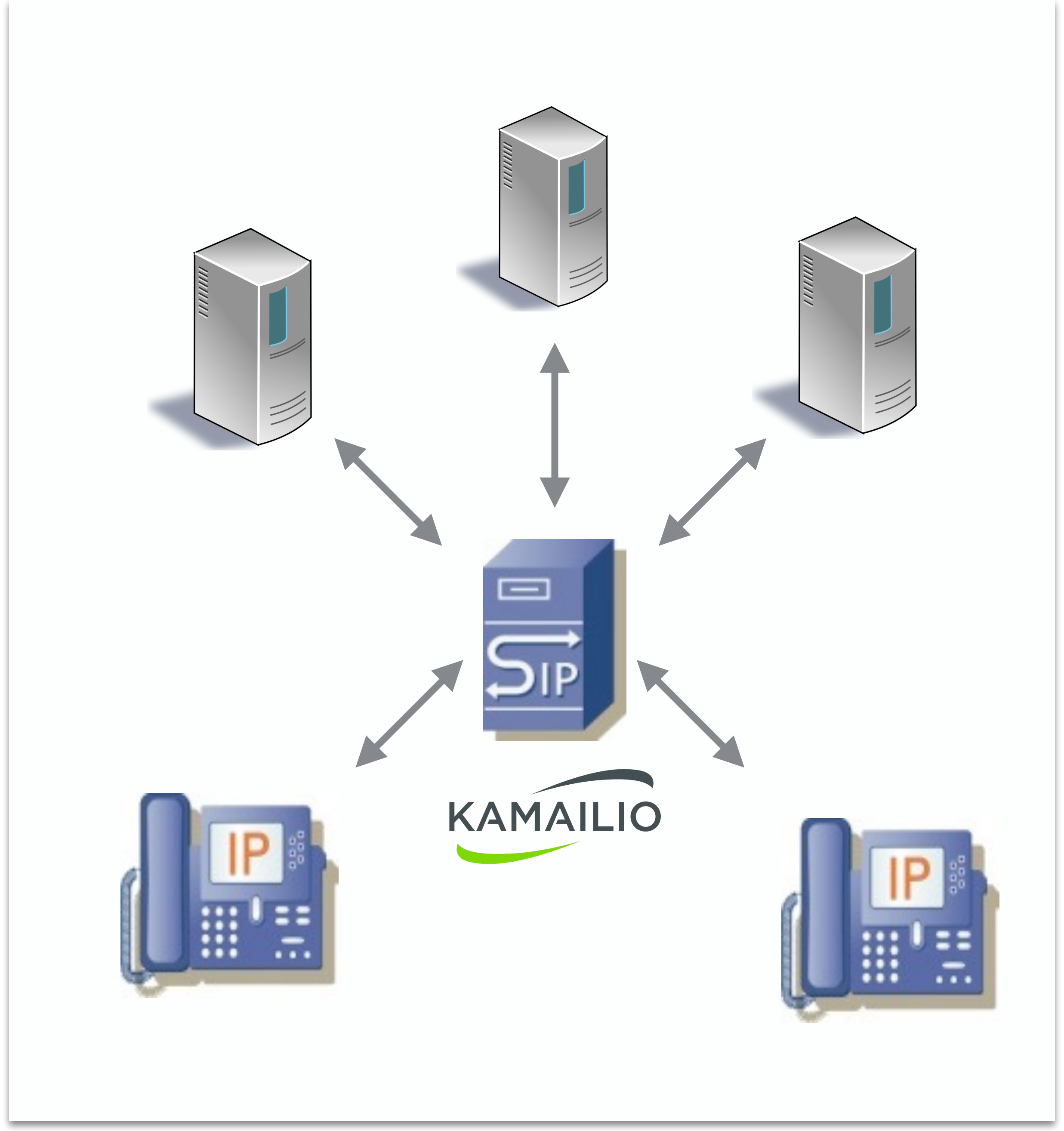
WHO AM I?

@MICONDA

- Originally from Romania, living in Berlin, Germany
- Computer science software engineer
- Involved in open source real time communications since 2002
- Shifted from a researcher position to professional consultancy for SIP, Kamailio and all RTC
- Developing and living only from open source software and services for more than 15 years
- C programmer - mainly VoIP server side infrastructure
- Co-founder and lead developer of Kamailio - www.kamailio.org
- Involved in a bunch of other open source projects
- Co-organizer of Kamailio World Conference
- Speaking and promoting OSS RTC at world wide events
- Enjoying sports and nature, both sea side and mountains
- Working at Asipto - www.asipto.com

KAMAILIO SIP SERVER IN ONE SLIDE

- Open Source SIP (IETF RFC3261) Signaling Server implementation, developed since 2001
- Can be used for VoIP (Voice, Video, VoLTE/IMS, SIP-I/SIP-T), Instant Messaging, Presence, WebRTC, IoT, Diameter, SQL and NoSQL backends, load balancing, least cost routing, security, …
- Designed for modularity, flexibility and scalability
  - used by large telecoms, mobile operators and OTT services world wide
  - thousands of call setups per second,
  - hundred thousands of connected phones per instance
- IPv6/IPv4 - UDP/TCP/TLS/SCTP/WebSocket - asynchronous routing
- Classic SIP - WebRTC gateway using Kamailio + RTPEngine
- Embedded interpreters: Lua, Python, JavaScript, Ruby, Squirrel, Perl, .Net, Java
- Over 250 modules (extensions) - https://www.kamailio.org/docs/modules/stable/
- Over 80 active developers each year
- Runs its own conference - Kamailio World
  - in Berlin, Germany: https://www.kamailioworld.com



New In Kamailio

2020 - 2021

V5.4.0 - NEW MODULES

- Major release v5.4.x - out in July 2020
  - dlgs - track dialogs in stateless mode and provide corresponding statistics
  - kafka - connector to Kafka server
  - pv_headers - flexible SIP header management with variables, simplifying configuration file
  - secsipid - implementation of STIR and SHAKEN IETF extensions, see RFC 8224 and RFC 8588 for details
  - systemdops - facilitate integration with systemd

KAMAILIO

https://www.kamailio.org/w/kamailio-v5-4-0-release-notes/

V5.4.0 - NEW FEATURES

- support for custom log engine - print log messages in structured JSON format
- options to load modules and set module parameters via command line
- ability to associate names to listen socket and use for routing rules
- keepalive done by usrloc to all registered contacts, with round trip measurement
- many new classes of variables - $xavu(…), $xavi(…), …
- ability to insert DNS records in cache at startup
- functions to encode/decode Contact address, to hide it behind server address
- added in-memory-only mode for presentity records
- tls enhancements: new variables, fine control on checking the peer certificate
- more control for siptrace auto-mirroring to sip uri, homer or to database
- event route execution on sipdump processing
- extensions to IMS/VoLTE extensions (ipsec, …)

KAMAILIO

https://www.kamailio.org/w/kamailio-v5-4-0-release-notes/

V5.5.0 - NEW IN DEVELOPMENT BRANCH

- To be released in 2021 - new additions in the last 2 months
  - sworker - new module for special tasks management
  - event_route[core:pre-routing]
  - option to store sip traffic in pcap files via sipdump
    - done also for TLS, but showing up as UDP for simplicity, with extra header metadata
  - event route to allow deciding what packets are mirrored by siptrace
    - rules based on IP addresses or headers content
  - support for histogram metrics for xhttp_prom (prometheus)
  - option to preserve contact user for topology stripping (topos)
  - rework of sip parser to use static map for standard headers
  - accounting records with local generated tags
  - new preprocessor directive $!defenv ID=ENVVAR
  - command line parameter --cfg-print to print config file after preprocessor directives evaluation
  - explode a string to XAVPs by delimiter
  - new transformations and variables

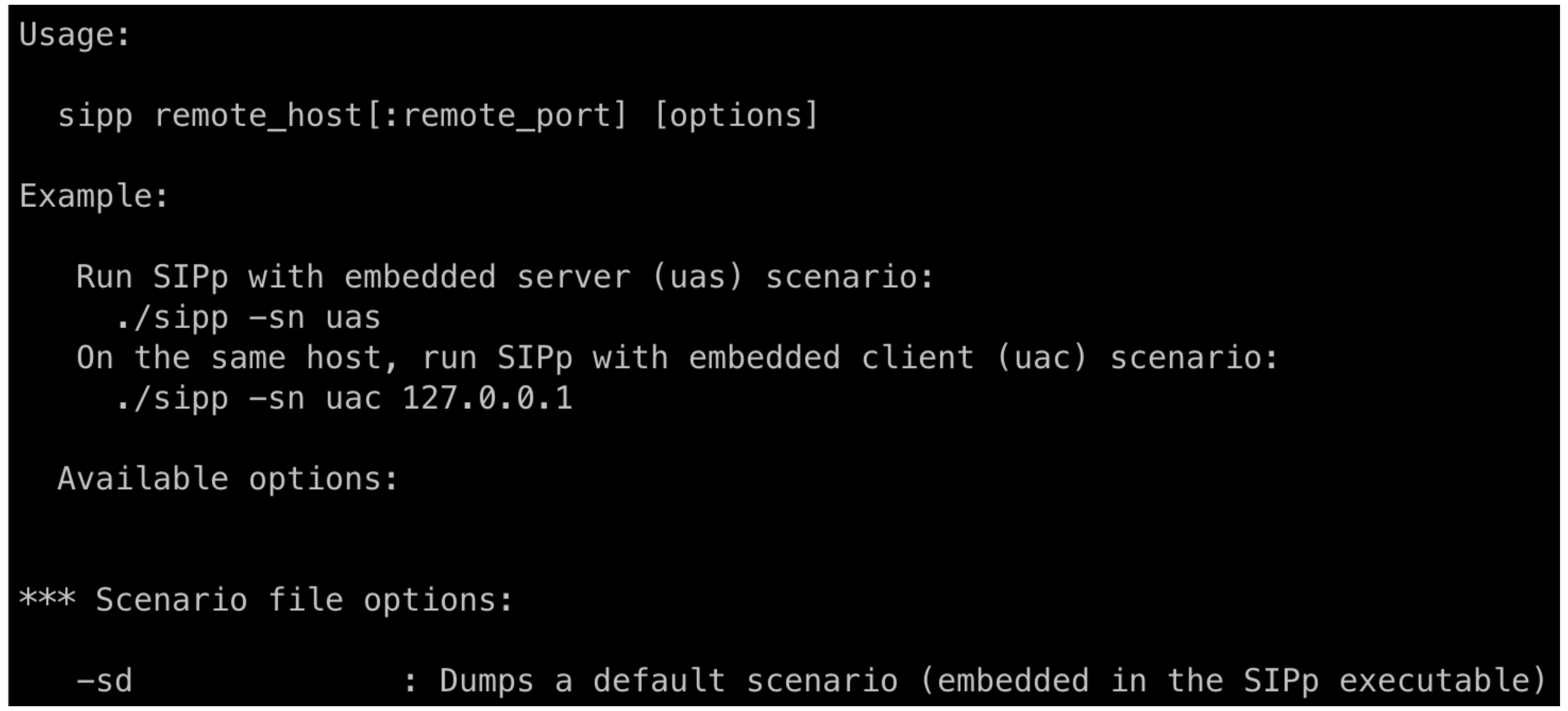
KAMAILIO

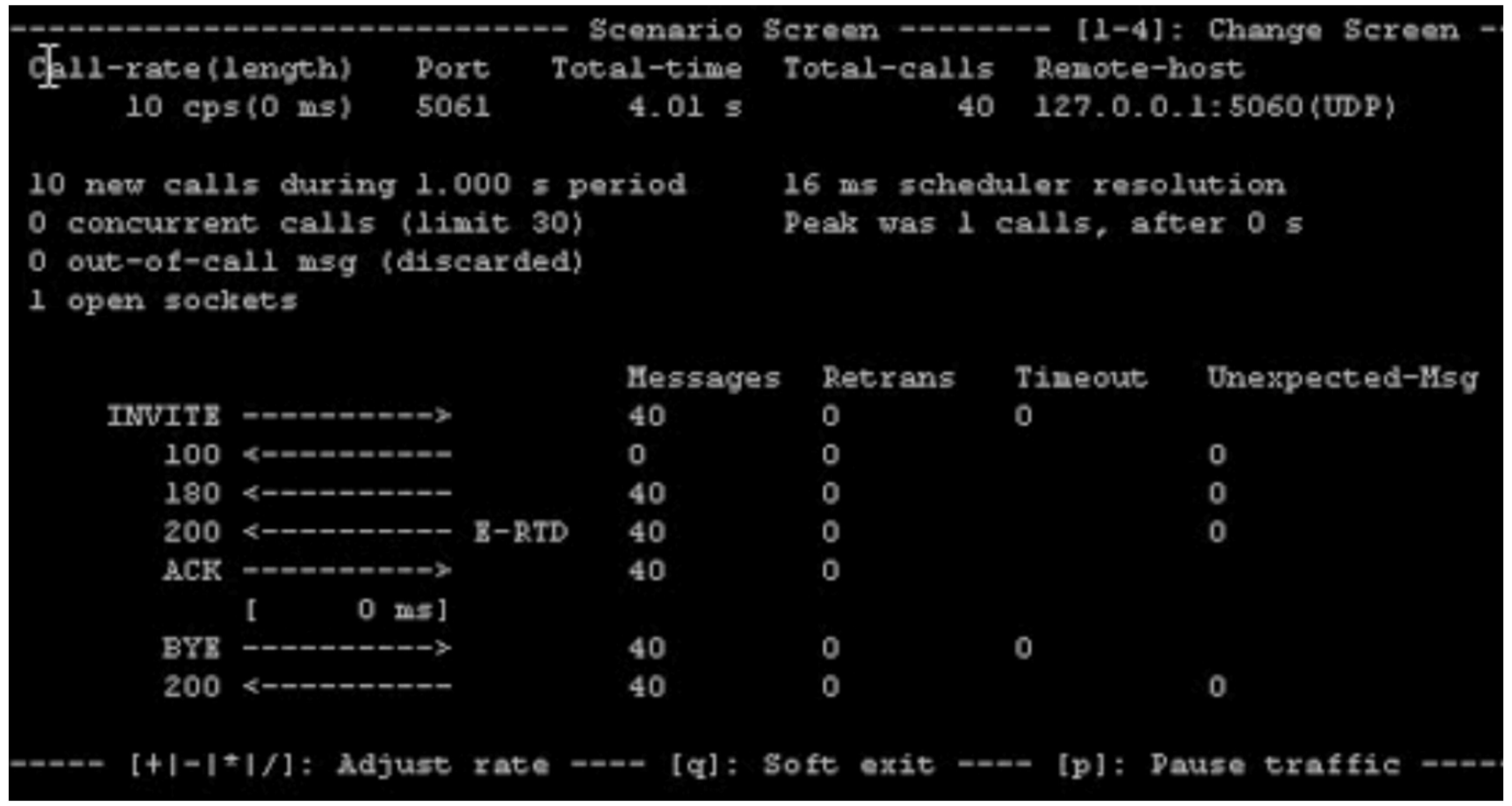
SIP Tools

Generate Traffic

SIPP

- the reference open source SIP performance testing
  - https://github.com/SIPp/sipp
  - packaged as sip-tester on Debian
  - generate and match SIP traffic based on XML scenarios
    - https://github.com/saghul/sipp-scenarios
    - https://github.com/pbertera/SIPp-by-example
  - SIP UAC behaviour
  - SIP UAS behaviour
    - SIPP (UAC) <=> SIP Proxy <=> SIPP (UAS}
  - can manage RTP traffic as well
  - See also
    - https://github.com/mojolingo/sippy_cup
    - generate SIPP scenarios





SIPSAK

- generate common SIP requests and scenarios from command line
  - https://github.com/nils-ohlmeier/sipsak
  - packaged on most of the Linux distros
  - send SIP OPTIONS ping requests
  - do user registration with authentication
  - simulate call to itself after registration
  - flooding or random users for stress testing
  - many options to set source or target numbers
  - send instant messaging

```
dublin@ireland:~$ sipsak -vv -s sip:88.99.225.41

message received:
SIP/2.0 200 Okey
Via: SIP/2.0/UDP 127.0.1.1:36295;branch=z9hG4bK.20d307d6;rport=47816;
From: sip:sipsak@127.0.1.1:36295;tag=7c62e8be
To: sip:88.99.225.41;tag=508f520dfecc7f66581e4edcefa359fe.7f5b561b
Call-ID: 2086856894@127.0.1.1
CSeq: 1 OPTIONS
P-Reason: keepalive
Server: kamailio (5.5.0-dev3 (x86_64/linux))
Content-Length: 0



** reply received after 22.646 ms **
   SIP/2.0 200 Okey
   final received
```

```
sipsak 0.9.7pre by Nils Ohlmeier
 Copyright (C) 2002-2004 FhG Fokus
 Copyright (C) 2004-2005 Nils Ohlmeier
 report bugs to nils@sipsak.org

 shoot  : sipsak [-f FILE] [-L] -s SIPURI
 trace  : sipsak -T -s SIPURI
 usrloc : sipsak -U [-I|M] [-b NUMBER] [-e NUMBER] [-x NUMBER] [-z NUMBER] -s SIPURI
 usrloc : sipsak -I|M [-b NUMBER] [-e NUMBER] -s SIPURI
 usrloc : sipsak -U [-C SIPURI] [-x NUMBER] -s SIPURI
 message: sipsak -M [-B STRING] [-O STRING] [-c SIPURI] -s SIPURI
 flood  : sipsak -F [-e NUMBER] -s SIPURI
 random : sipsak -R [-t NUMBER] -s SIPURI

 additional parameter in every mode:
   [-a PASSWORD] [-d] [-i] [-H HOSTNAME] [-l PORT] [-m NUMBER] [-n] [-N]
   [-r PORT] [-v] [-V] [-w]

  -h                 displays this help message
```

SIPVICIOUS - AKA FRIENDLY-SCANNER

- a set of security tools that can be used to audit SIP based VoIP systems
  - https://github.com/EnableSecurity/sipvicious
  - svmap - SIP scanner
  - svwar - identifies working extension lines on a PBX
  - svcrack - password cracker making use of digest authentication
  - svreport - manage sessions and write reports
  - svcrash - kill old versions of svwar and svcrack

SIPVICIOUS

```
mirko@mirko-VirtualBox/pentest/voip/sipvicious$ ./svmap.py 192.168.101.* -m INVITE
| SIP Device            | User Agent                        | Fingerprint                                                      |
------------------------------------------------------------------------------------------------------------------------------------
| 192.168.101.105:5060  | Asterisk PBX 1.6.2.24             | Asterisk / Linksys/PAP2T-3.1.15(LS) / Asterisk PBX               |
| 192.168.101.105:37268 | Z 3.2.21357 r21103                | 3CXPhoneSystem / AVM FRITZ!Box Fon WLAN 7170 29.04.22 (Sep       |
|                       |                                   | 6 2006) / T-Com Speedport W500V / Firmware v1.37                 |
|                       |                                   | MxSF/v3.2.6.26                                                   |
| 192.168.101.190:5060  | X-Lite release 4.5.5  stamp 71236 | AVM or Speedport                                                 |
| 192.168.101.108:47723 | Z 3.2.21357 r21103                | 3CXPhoneSystem / AVM FRITZ!Box Fon WLAN 7170 29.04.22 (Sep       |
|                       |                                   | 6 2006) / T-Com Speedport W500V / Firmware v1.37                 |
|                       |                                   | MxSF/v3.2.6.26                                                   |
```

SIPPTS

- another set of tools to audit VoIP servers and devices using SIP protocol
  - https://github.com/Pepelux/sippts
  - among the tools
  - *Sipscan* - a fast scanner for SIP services
  - *Sipexten* - identifies extensions on a SIP server.
  - *Sipcracker* - a remote password cracker.
  - *Sipinvite* - checks if a server allow us to make calls without authentication

```
pepelux@debian:~/sippts$ perl sipscan.pl -h pepelux -ua test -cd mydomain -proto tls
IP address      Port    Proto   User-Agent
==========      ====    =====   ==========
185.XXX.YYY.210 5061    tls     Kamailio Proxy

pepelux@debian:~/sippts$ perl sipscan.pl -h pepelux -ua test -cd mydomain -proto all
IP address      Port    Proto   User-Agent
==========      ====    =====   ==========
185.XXX.YYY.210 5060    tcp     Kamailio Proxy
185.XXX.YYY.210 5060    udp     Kamailio Proxy
185.XXX.YYY.210 5061    tls     Kamailio Proxy
```

KALI LINUX

- Kali Linux is a Debian-derived Linux distribution
  - designed for digital forensics and penetration testing
  - many tools related to SIP and VoIP
  - https://tools.kali.org/tools-listing

SIPPING

- SIPPing is a simple SIP packet forging tool written in pure Python
  - https://github.com/pbertera/SIPPing
  - can create SIP Requests based on simple text templates
  - variables defined in command line that will be substituted in template

```
OPTIONS sip:%(user)s@%(destination)s:%(port)s;line=kutixubf SIP/2.0
Via: SIP/2.0/UDP 192.168.10.1:5060;branch=z9hG4bK001b84f6;rport
Max-Forwards: 70
From: "fake" <sip:fake@192.168.10.1>;tag=as2e95fad1
To: <sip:%(user)s@%(destination)s:%(port)s;line=kutixubf>
Contact: <sip:fake@192.168.10.1:5061>
Call-ID: 7066d2f12e6f22ec1dc1231f4cade6be@172.16.18.40:5060
User-Agent: SIPPing
Date: Wed, 24 Apr 2013 20:35:23 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH
Supported: replaces, timer
```

```
sipping.py -r test-template.txt -d 172.16.18.35 -p 5060 -S 172.16.18.90  -P 5061 -c 3 -vuser:120 -v destination:192.168.20.1 -v port:5060
```

WSCTL

- cli tool written in Go to connect to SIP servers via websocket
  - https://github.com/miconda/wsctl
  - can create SIP Requests based on templates
  - variables defined in JSON files or via command line parameters
  - support for digest authentication
  - Internal variable substitution

```
go run wsctl.go \
   --url='wss://myserver.com:8443/ws' \
   --template=examples/options-aa-tpl.sip \
   --fields=examples/options-aa-fld.json \
   --auser='test' --apasswd='secret'
```

```
OPTIONS sip:{{.callee}}@{{.domain}} SIP/2.0
Via: SIP/2.0/WSS df7jal23ls0d.invalid;branch=z9hG4bKasudf-3696-24845-1
From: "{{.caller}}" <sip:{{.caller}}@{{.domain}}>;tag={{.fromtag}}
To: "{{.callee}}" <sip:{{.callee}}@{{.domain}}>
Call-ID: {{.callid}}
CSeq: {{.cseqnum}} OPTIONS
Subject: testing
Content-Length: 0
```

```
{
        "caller": "alice",
        "callee": "bob",
        "domain": "localhost",
        "fromtag": "$uuid",
        "callid": "$uuid",
        "cseqnum": "$randseq"
}
```

VOIP_PATROL - VOIP_PERF

- voip_patrol
  - https://github.com/jchavanton/voip_patrol
  - VoIP signaling and media test automation
  - Follows a scenario in XML format and will output results in JSON
- voip_perf
  - https://github.com/jchavanton/voip_perf
  - a SIP signalling performance testing application that can provide a server and a client

OSIP - EXOSIP - SIP_MONITOR

- sip_monitor
  - https://git.savannah.nongnu.org/git/exosip.git
  - part of libexosip, built on top of libosip
  - small cli tool mainly useful for doing registrations over TLS

```
sip_monitor -r sip:openrcs.com -u sip:alice@openrcs.com -U alice -P SECRET -t TLS -s --outbound "<sip:sip.openrcs.com;lr>"
```

CLI SIP PHONES

- baresip
  - https://github.com/baresip/baresip
  - a portable and modular SIP User-Agent with audio and video support

- pjsua
  - https://www.pjsip.org/pjsua.htm
  - an open source command line SIP user agent using PJSIP stack

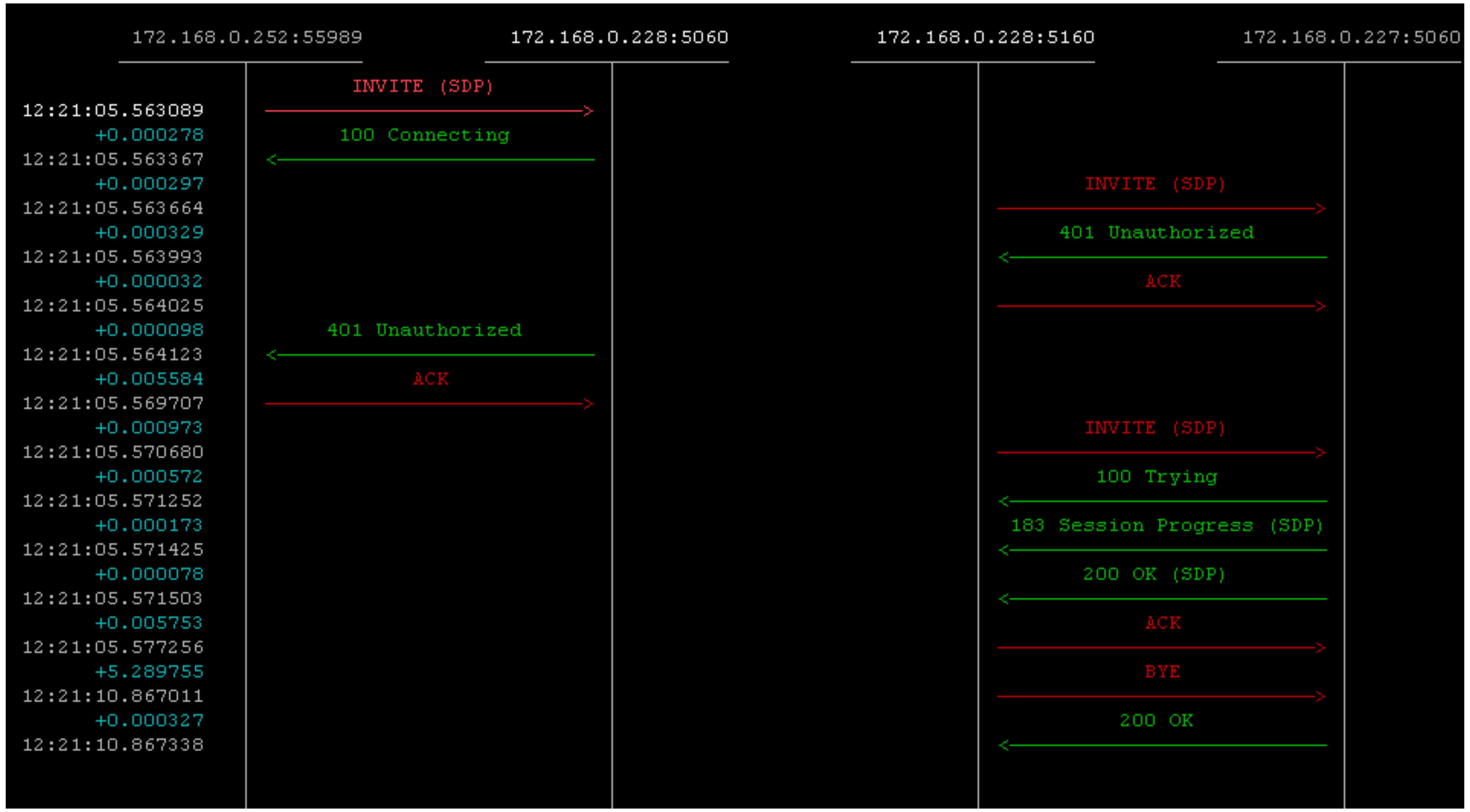
SIP Tools

Analyze Traffic

SNGREP

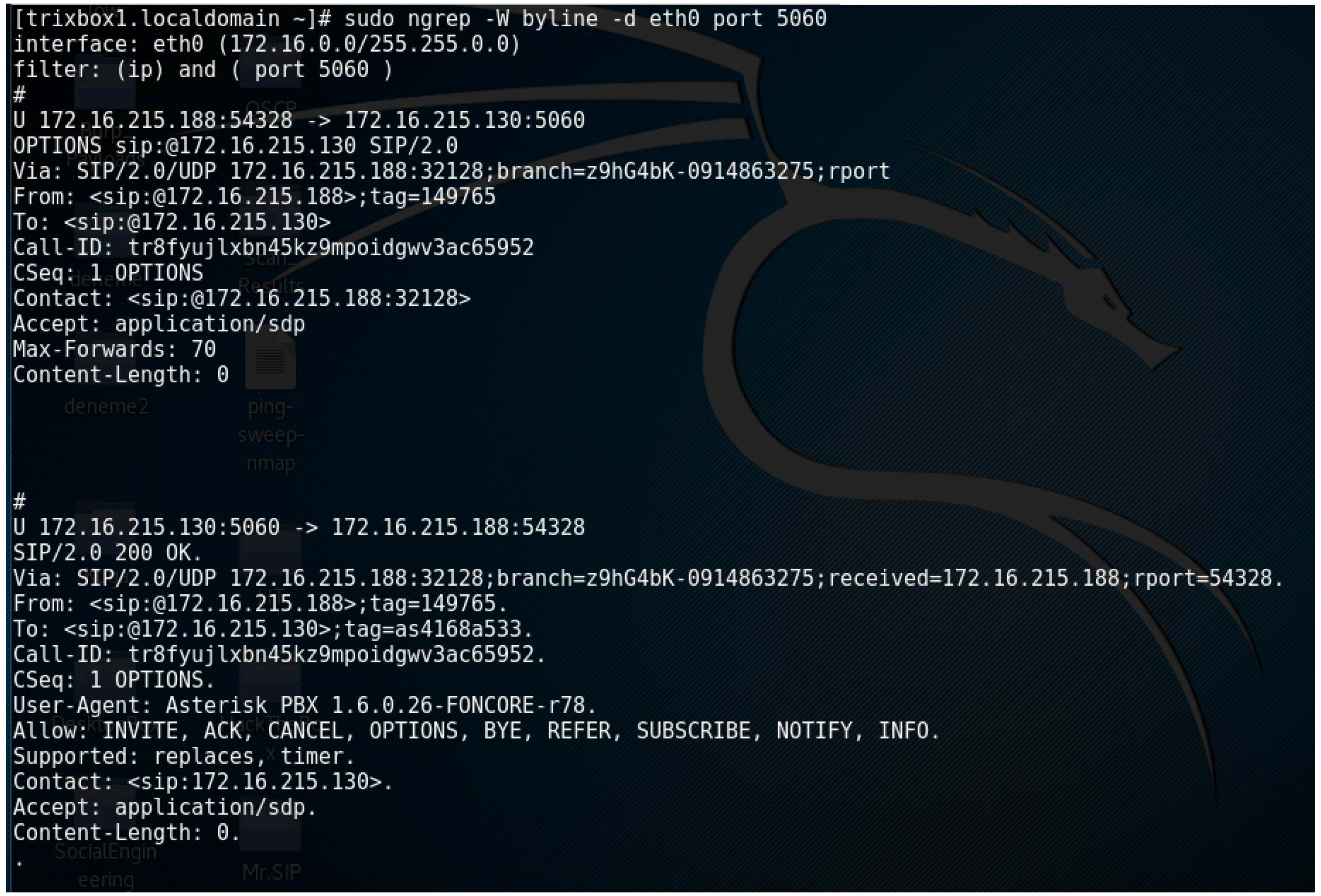
- sngrep is a tool for displaying SIP calls message flows from terminal
- live capture to display realtime SIP packets or PCAP viewer
  - https://github.com/irontec/sngrep

Sngrep



NGREP

- like GNU grep applied to the network layer
- live capture to display realtime SIP packets, also a PCAP viewer
    - https://github.com/jpr5/ngrep



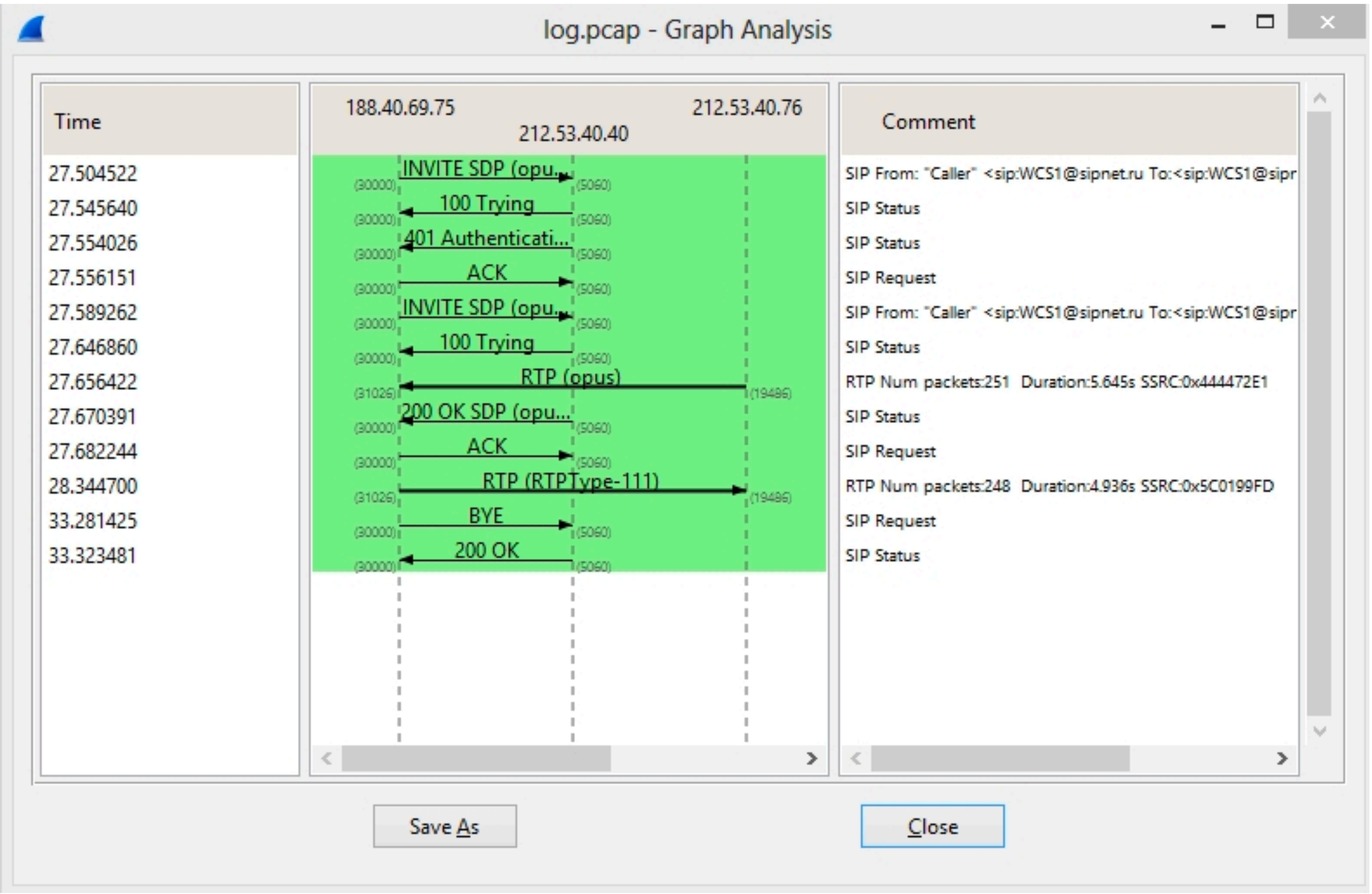
SIPGREP

- similar to grep targeting SIP packets that highlights important message attributes
  - https://github.com/sipcapture/sipgrep

```
root@voip ~ # sipgrep
interface: eth0 (158.193.152.0/255.255.255.128)
filter: (ip or ip6) and ( portrange 5060-5061) or (udp and ip[6:2] & 0x3fff != 0)

U 2019/10/24 14:54:19.710052 158.193.139.84:5060 -> [redacted]5060

REGISTER sip:158.193.152.10 SIP/2.0.
Via: SIP/2.0/UDP 158.193.139.84:5060;branch=z9hG4bK34ab4961.
From: <sip:312@[redacted]>;tag=000d28e80caebfe94ed6a6ce-7fad4c46.
To: <sip:312@[redacted].
Call-ID: 000d28e8-0cae0005-1867171c-61346c35@158.193.139.84.
Max-Forwards: 70.
Date: Thu, 24 Oct 2019 12:54:20 GMT.
CSeq: 87742 REGISTER.
User-Agent: Cisco-CP7960G/8.0.
Contact: <sip:312@158.193.139.84:5060;user=phone;transport=udp>;+sip.instance="<urn:uuid:00000000-0000-0000-000
0-000d28e80cae>";+u.sip!model.ccm.cisco.com="7".
Content-Length: 0.
Expires: 120.
.


U 2019/10/24 14:54:19.710798 [redacted]:5060 -> 158.193.139.84:5060

SIP/2.0 401 Unauthorized.
Via: SIP/2.0/UDP 158.193.139.84:5060;rport=5060;received=158.193.139.84;branch=z9hG4bK34ab4961.
Call-ID: 000d28e8-0cae0005-1867171c-61346c35@158.193.139.84.
From: <sip:312@[redacted]>;tag=000d28e80caebfe94ed6a6ce-7fad4c46.
To: <sip:312@[redacted]>;tag=z9hG4bK34ab4961.
CSeq: 87742 REGISTER.
WWW-Authenticate: Digest realm="kis.fri.uniza.sk",nonce="1571921659/125af93e7c0fb4d2690fe820d1d2f019",opaque="3
```

MORE CLI TOOLS

- tshark - part of WireShark project
- WireShark is the most well know packet analyzer application
  - very good support for SIP and VoIP (parsing, diagram flow, play RTP audio, …)
  - https://www.wireshark.org/docs/man-pages/tshark.html
  - https://www.wireshark.org/



- tcpdump - the grandfather of packet capture
  - https://www.tcpdump.org/

SIP Tools

Kamailio Project

PROTOSHOOT

- send SIP messages from a file via UDP, TCP or SCTP
  - https://github.com/kamailio/kamailio/tree/master/misc/tools/protoshoot

```
version: protoshoot 0.4
Usage: protoshoot -f file -d address -p port -c count [-v]
Options:
    -f file       file with the content of the udp packet (max 65k)
    -d address    destination address
    -p port       destination port
    -c count      number of packets to be sent
    -s usec       microseconds to sleep before sending "throttle" packets
    -t throttle   number of packets to send before sleeping
    -r            sleep randomly up to -s usec packets (see -s)
    -T            use tcp instead of udp
    -S            use sctp instead of udp
    -1            use sctp in one to one mode
    -n no         tcp connection number
    -R            close the tcp connections with RST (SO_LINGER)
    -v            increase verbosity level
    -V            version number
    -h            this help message
```

MODULES

- *siptrace* - save SIP traffic to database or mirror the traffic to another system (e.g., one running sipcature module)
  - https://www.kamailio.org/docs/modules/stable/modules/siptrace.html
- *sipcapture* - save mirrored SIP traffic to backend
  - https://www.kamailio.org/docs/modules/stable/modules/sipcapture.html
  - (see also sipcapture.org project)
- *sipdump* - write SIP traffic to text or pcap file or both
  - saves also Kamailio runtime metadata (e.g., list of processes, …)
  - https://www.kamailio.org/docs/modules/stable/modules/sipdump.html

KAMAILIO

Soon 20 Years Of Development

THANK YOU!

Daniel-Constantin Mierla

Co-Founder Kamailio Project

@miconda

asipto.com

KAMAILIO WORLD
CONFERENCE & EXHIBITION

www.kamailioworld.com