

How to debug, troubleshoot and monitor VoIP using MikroTik



Whoami

- Voicenter
- Homer

Voip Protocols

- SIP
- RTP
- RTCP

Mikrotik VoIP Setup

- QOS
- Provisioning
- Monitoring

Tools for VoIP Analytics

- Wireshark
- Sngrep
- CaptAgent
- RtpAgent

Homer Cloud

- Troubleshooting
- Monitoring
- Alerting

whoami <

Shlomi Gutman

CTO of **Voicenter** (Israel)

VP of Cloud Products at **QXIP** (Amsterdam)



whoami <

HI.

Shlomi Gutman.

Founder and CTO at Voicenter.

Open-Source Telephony expert.

Built my first computer when I was 7 years old.



shlomi@voicenter.com



whoami <

Voicenter is A leading **telecommunication technology company** providing top-tier business telephony since 2007

We are delivering a 'One-stop-shop' solution for business all around the world



**Telecom
Services**



PBX



**Call
Center
Solution**

Voicenter – Cloud Contact Center

- Cloud-based Phone system
- Hybrid Solution
- Real Time Dashboards
- Workforce Management
- Dialers
- Api
- Integration

Voicenter – Cloud Contact Center

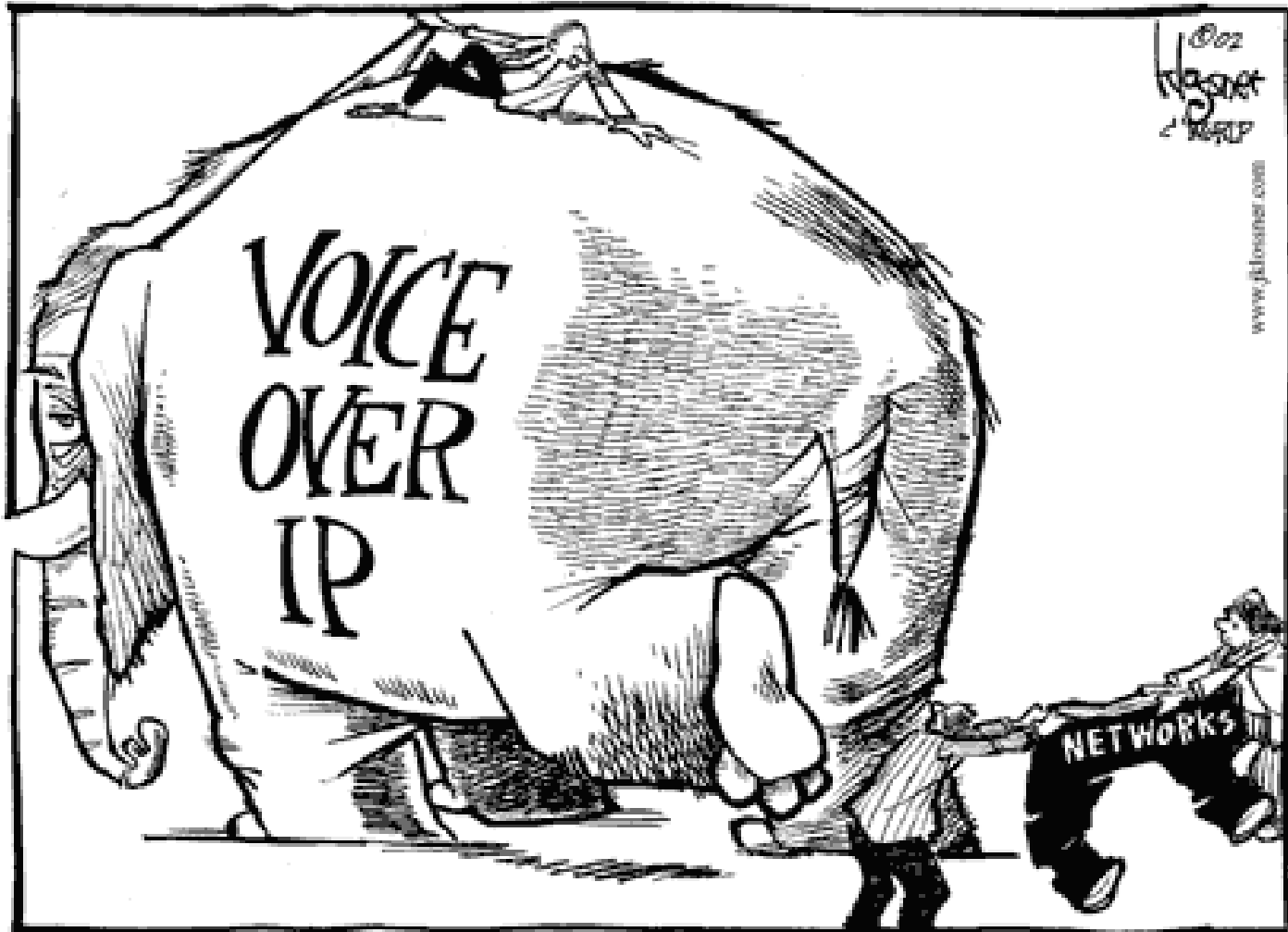
Voicenter is an Israel based business providing a solid array of services to its customers, including:

- Cloud based Phone Systems
- Hybrid Solutions
- Real Time Dashboards
- Workforce Management
- Dialers
- Api
- Integration

QXIP BV is an Amsterdam based R&D Company specializing in *Open-Source* and *Commercial Voice* Technologies deployed and trusted by thousands of businesses worldwide, include large telephony and network operators, voice service carriers, voip service providers, cloud service providers, call center operators and voice equipment vendors.

QXIP Capture Technologies are natively implemented in all major OSS voip platforms such as *Kamailio*, *OpenSIPS*, *FreeSWITCH*, *Asterisk*, *RTPEngine* and many tools such as *sipgrep*, *sngrep*.

Elephant in the server room



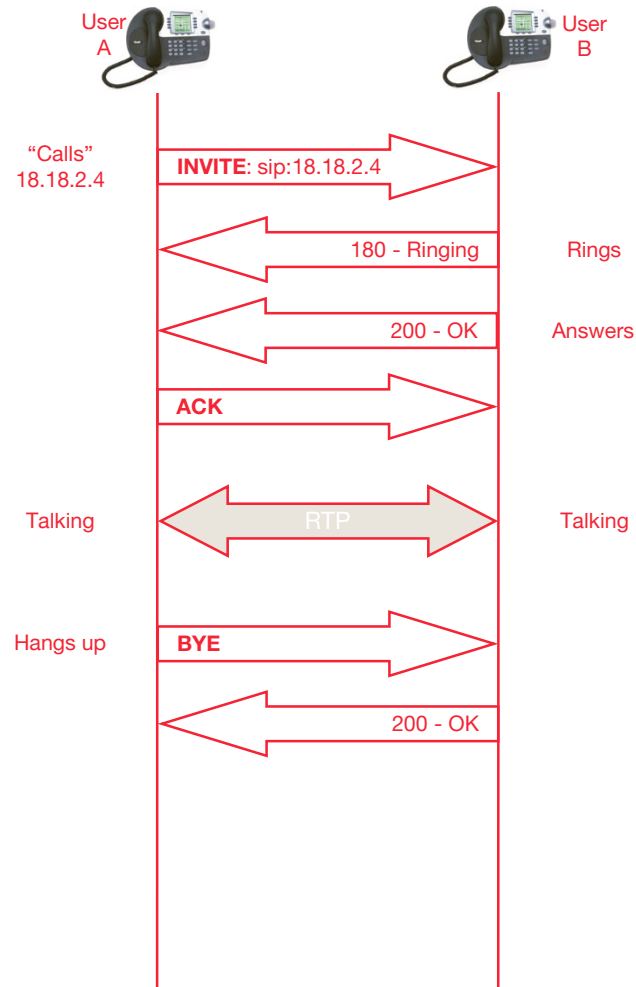
VoIP & RTC Problems

- Connectivity Problems
- Call Quality Problems
- Security Problems
- Multi Equipment management
- Hard to troubleshoot
- Mission Critical Application

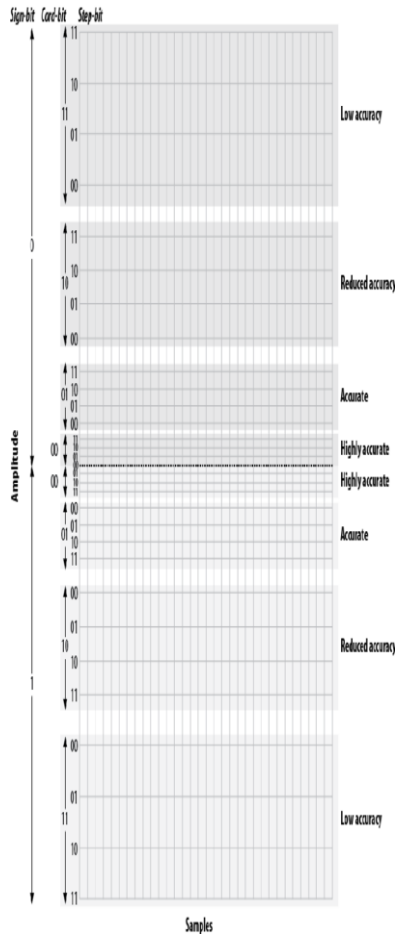
VoIP Protocols

- SIP / WEBRTC / TLS – Signaling Protocols
- RTP - Media Protocol
- RTCP – Real Time Control Protocol

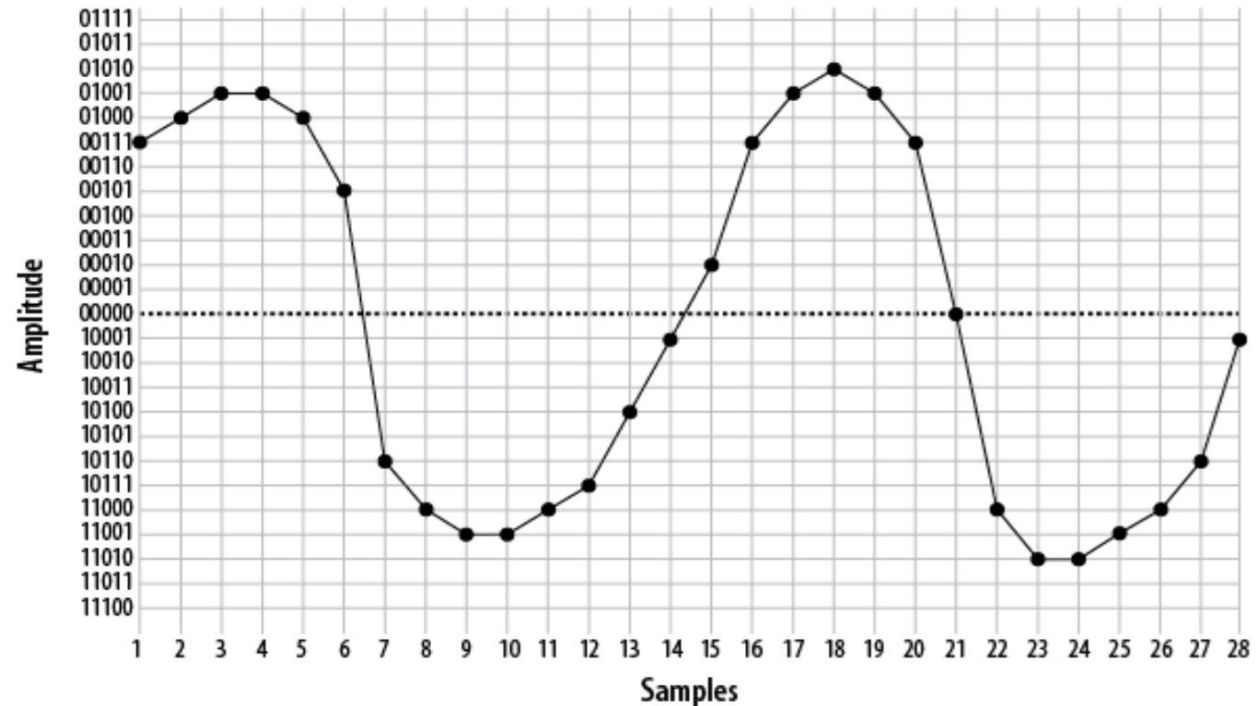
SIP Flows - Basic



RTP - *How Digital Audio Works*



00111 01000 01001 01001 01000 00101 10110 11000 11001
11001 11000 10111 10100 10001 00010 00111 01001 01010
01001 00111 00000 11000 11010 11010
11001 11000 10110 10001



RTCP-RTP (Quality) Control Protocol

```
"event": {  
  "media": "audio",  
  "base": 48000,  
  "lsr": 37971368,  
  "lost": 0,  
  "lost-by-remote": 0,  
  "jitter-local": 18940,  
  "jitter-remote": 0,  
  "packets-received": 39,  
  "packets-sent": 40,  
  "bytes-received": 6708,  
  "bytes-sent": 7280  
}
```

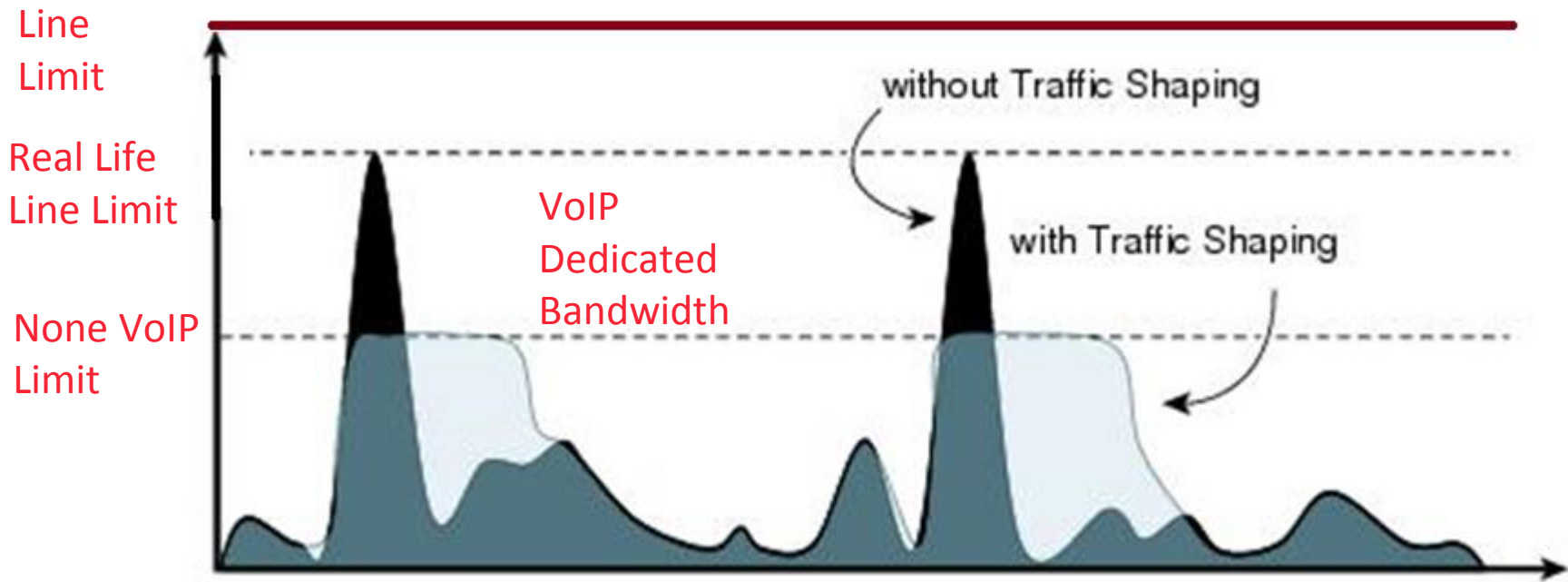


1 RTCP packet per RTP stream each 5-10 seconds

How Can Mikrotik Push my Voip Packets ?



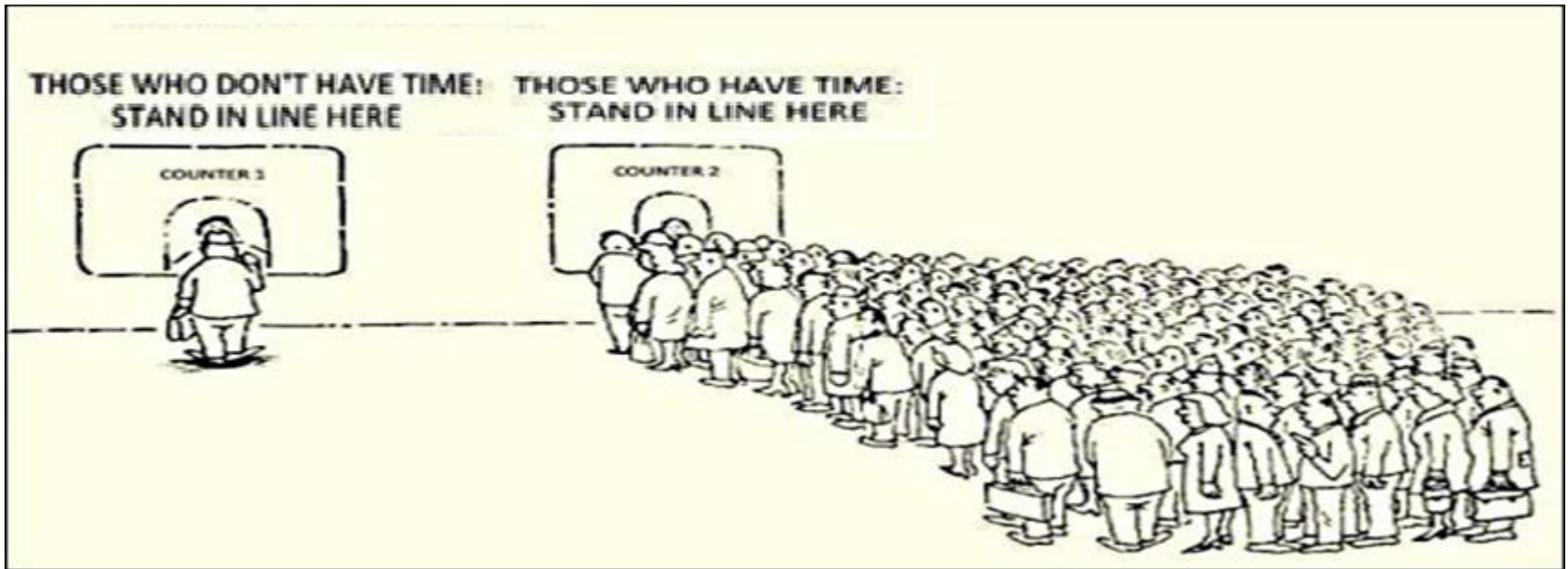
Traffic Shaping Concept



Losers make promises they often break.
Winners make commitments they always keep.

VoIP QoS Best Practice

- Address List Maintenance
- Connection Marking
- Packet Marking
- Queues configuring



Media servers Import Script

Script <MediaServersImport>

Name: MediaServersImport

Owner: admin

Policy: ☐ ftp ☐ reboot
☒ read ☒ write
☒ policy ☐ test
☐ password ☐ sniff
☐ sensitive ☐ romon
☐ dude

Last Time Started:

Run Count: 0

```
{:do {  
/tool fetch url=" http://mikrotik.XXXX.com/script/MediaServer.rsc" mode=http  
} on-error={ :put "Error on downloading OF MediaServer Script -> http://mikrotik.XXXX.com/script/IPList/MediaServer.rsc";  
#Start Loading  
:do {  
/import file-name=MediaServer.rsc  
} on-error={ :put "Error on Runing MediaServer.rsc";}]
```

Media servers HTTP Response

```
:put " * *****Add XX.XX.XX.XX MGW 01 to MediaServer*****"  
:do {  
  /ip firewall address-list add address=XX.XX.XX.XX  
list=MediaServerList comment="MGW 01 ->MediaServer"  
  } on-error={ :put " Failed to add XX.XX.XX.XX MGW 01 to  
MediaServer probably already there "};
```

```
:put " * *****Add XX.XX.XX.XX MGW 01 to MediaServer*****"  
:do {  
  /ip firewall address-list add address=XX.XX.XX.XX  
list=MediaServerList comment="MGW 01 ->MediaServer"  
  } on-error={ :put " Failed to add XX.XX.XX.XX MGW 01 to  
MediaServer probably already there "};
```

Connection Marking

New Mangle Rule

General Advanced Extra Action Statistics

Chain: prerouting

Src. Address:

Dst. Address:

Protocol: ☐ udp

Src. Port:

Dst. Port: ☐ 5060,5061,10000-32767

Any. Port:

P2P:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State: ☐ invalid ☐ established ☐ related ☒ new

General Advanced Extra Action Statistics

Src. Address List:

Dst. Address List: ☐ MediaServerList

Layer7 Protocol:

Content:

General Advanced Extra Action Statistics

Action: mark connection

☐ Log

Log Prefix:

New Connection Mark: VoipTrafficConnectionMark

☒ Passthrough

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Pocket Marking

New Mangle Rule

General

Advanced

Extra

Action

Statistics

Chain: prerouting

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark: VoipTrafficConnectionMark

Routing Mark:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Mangle Rule <>

General

Advanced

Extra

Action

Statistics

Action: mark packet

☐ Log

Log Prefix:

New Packet Mark: NonVoipPacketMark

☒ Passthrough

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Queue for non voip traffic

Simple Queue <NonVoipTrafficQueue>

General Advanced Statistics Traffic Total ...

Name: NonVoipTrafficQueue

Target: pppoe-out1

Dst.:

Target Upload Target Download

Max Limit: 3M 20M bits/s

Burst

Burst Limit: unlimited unlimited bits/s

Burst Threshold: unlimited unlimited bits/s

Burst Time: 0 0 s

Time

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Torch

New Simple Queue

General Advanced Statistics Traffic Total Total Statistics

Packet Marks: NonVoipPacketMark

OK

Cancel

Apply

VoIP Monitoring Using Mikrotik



Switch Layer
mirroring

Good Performance

Packet Sniffer stream

Bad Performance

Pcap File analytics

Ugly from any perspective

Switch Layer mirroring

admin@192.168.13.1 (MikroTikMikroTikBridgeBO) - WinBox v6.34.2 on hAP lite (smips)

Session Settings Dashboard

Safe Mode Session: 192.168.13.1

RouterOS WinBox

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
Make Supout.rtf
Manual
New WinBox
Exit

Switch

Switch Port Host VLAN Rule

Find

Name	Type	Mirror Source	Mirror Target
switch1	Atheros 8227	ether3	ether1

Switch <switch1>

Name: switch1

Type: Atheros 8227

Mirror Source: ether3

Mirror Target: ether1

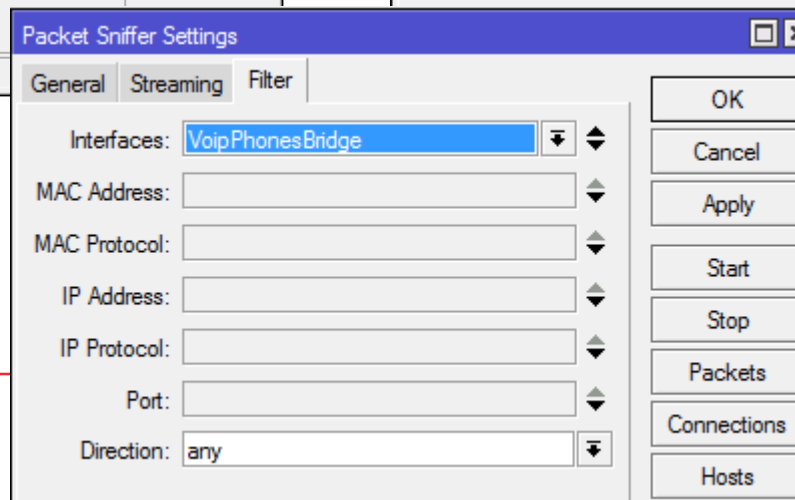
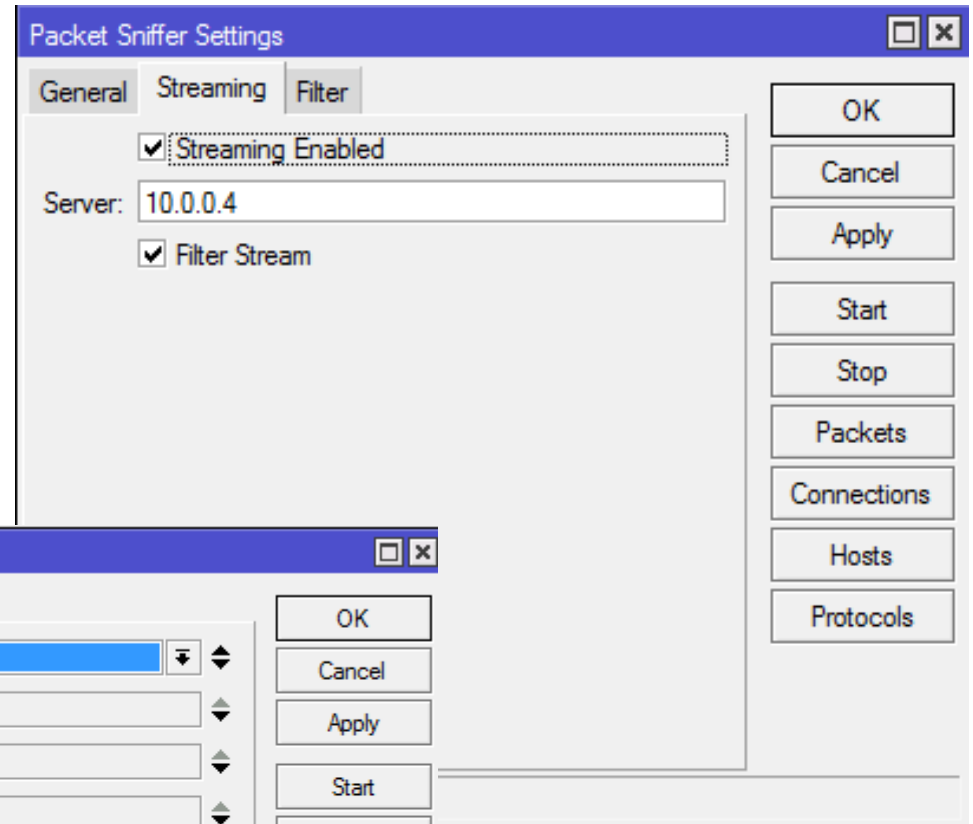
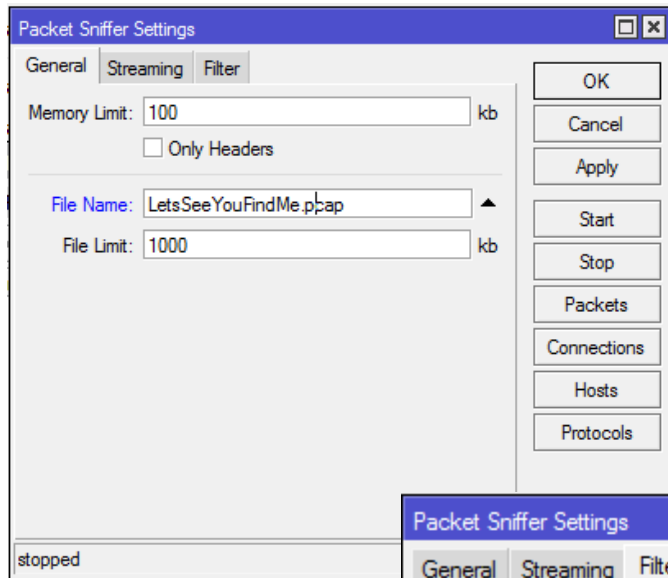
☐ Switch All Ports

OK
Cancel
Apply

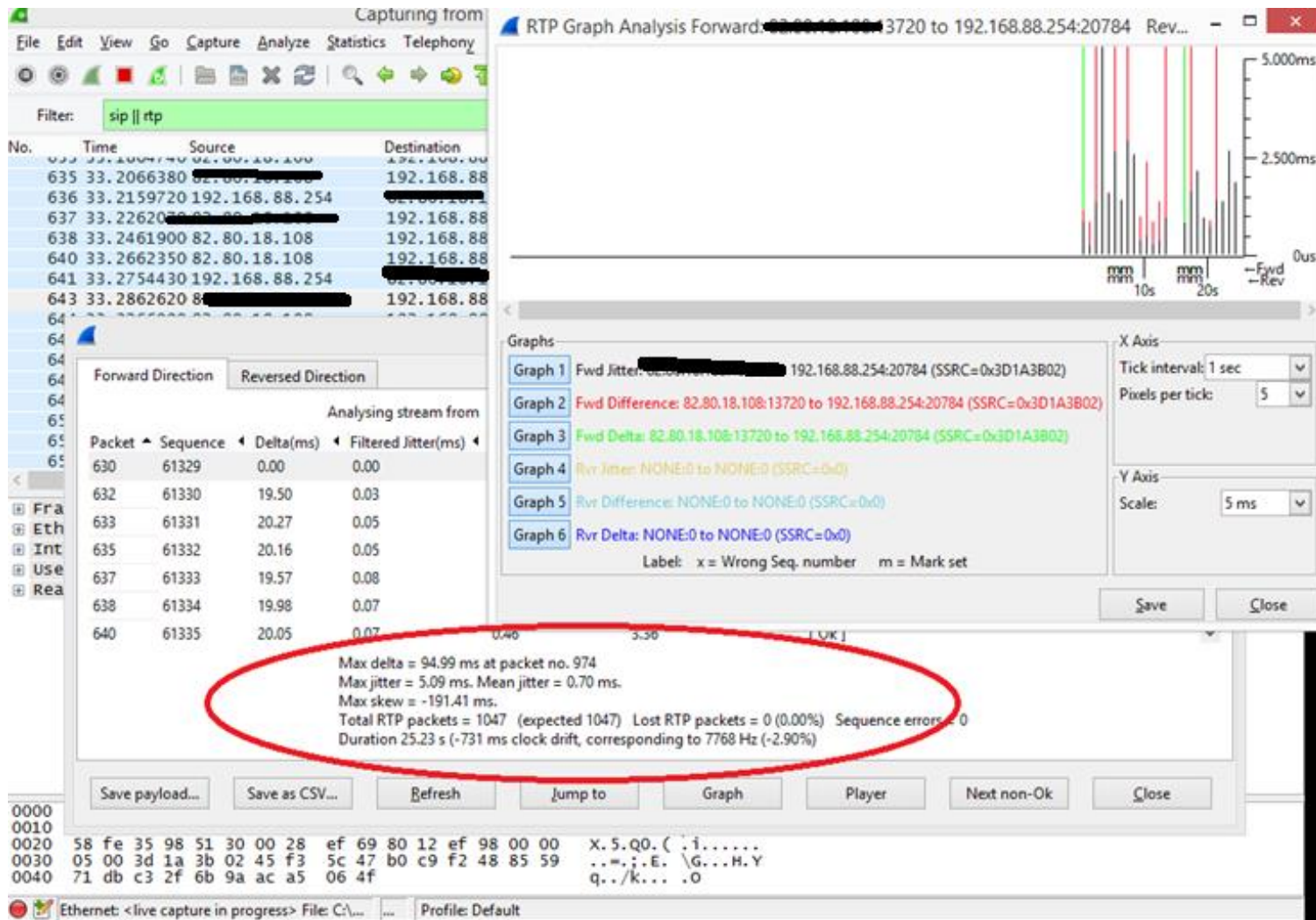
1 item (1 selected)

Packet Sniffer Setup

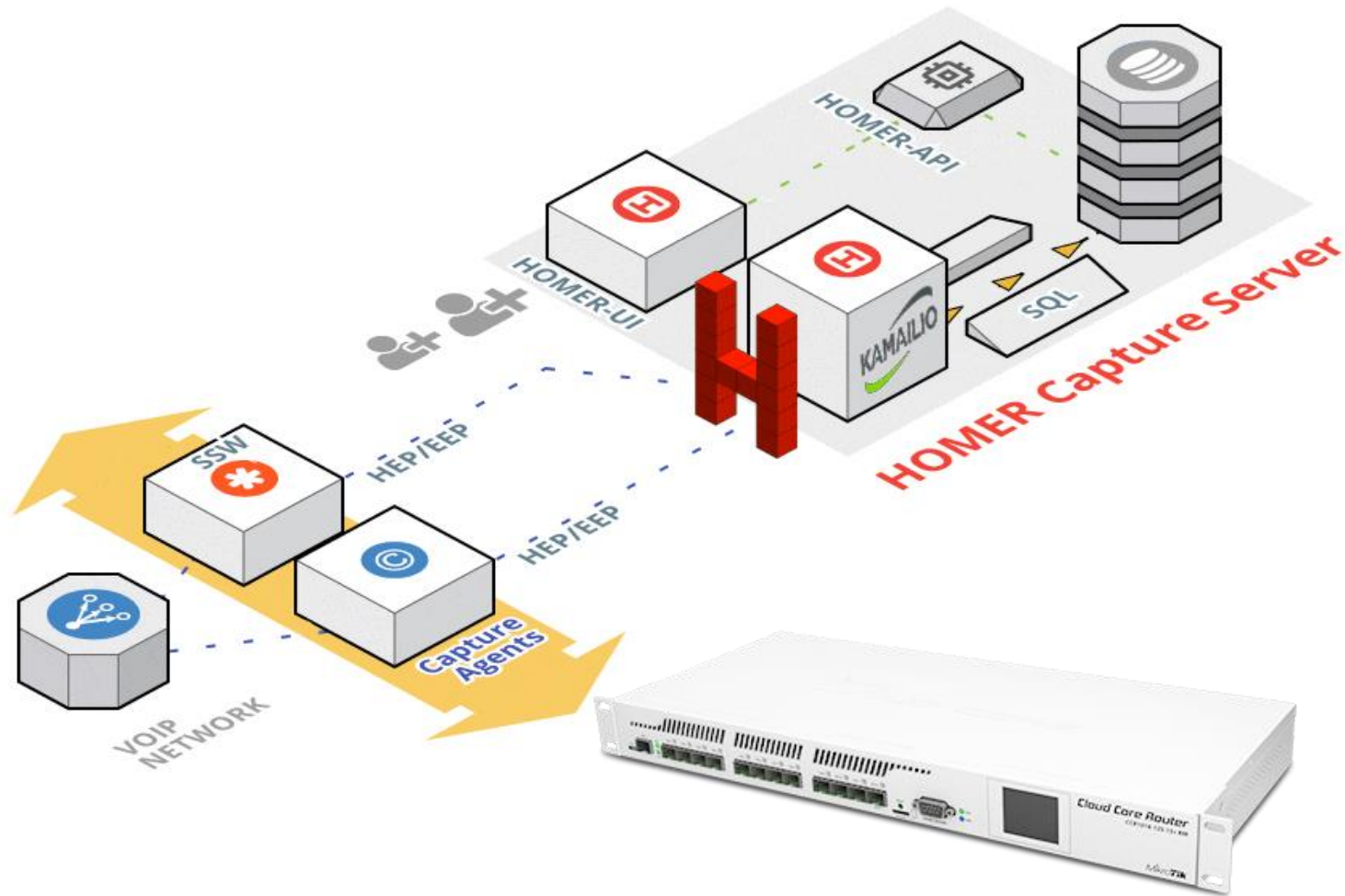
(TZSP - Packet Sniffer encapsulation)



RTP in Wireshark



SIP + RTP in HOMER Cloud

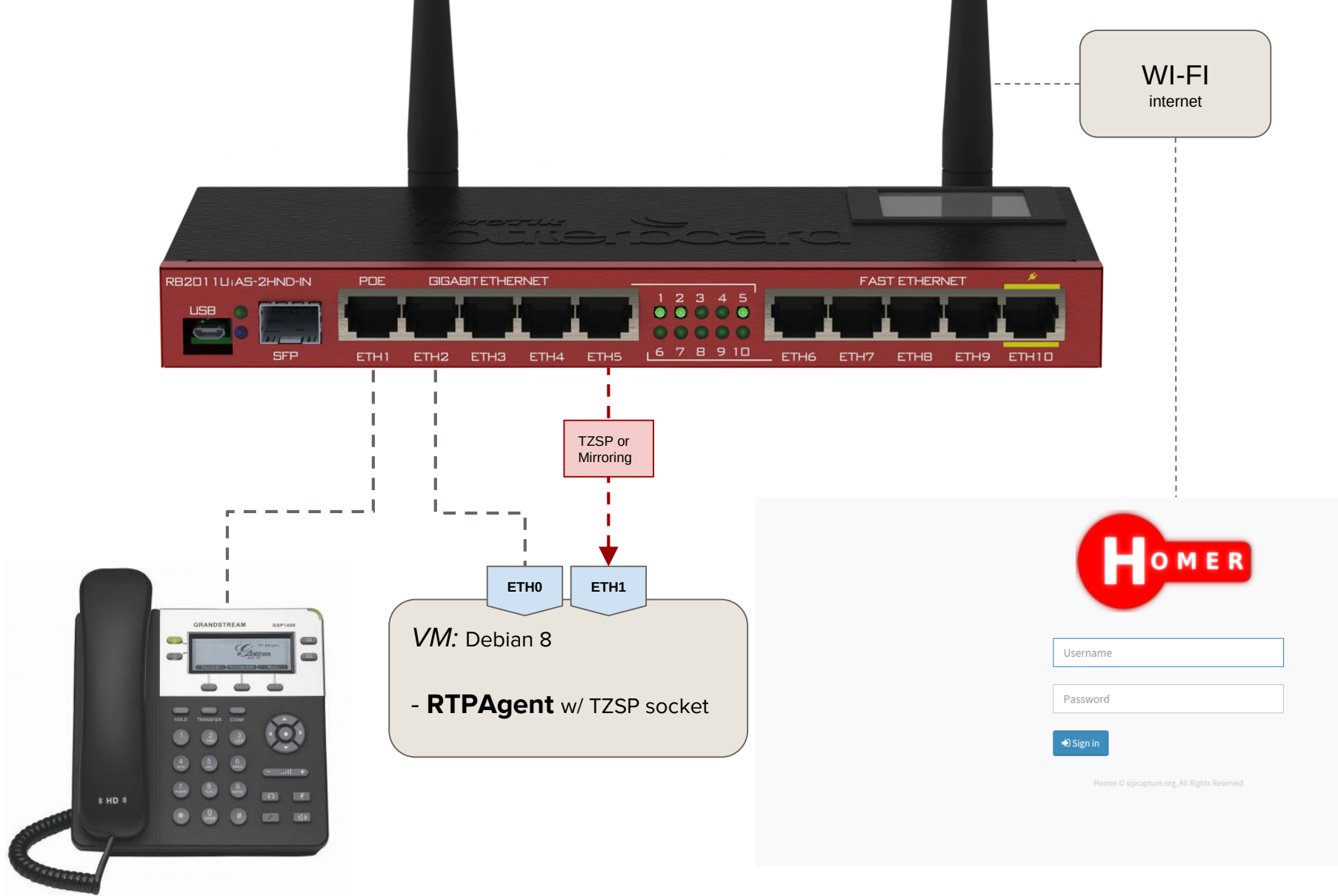


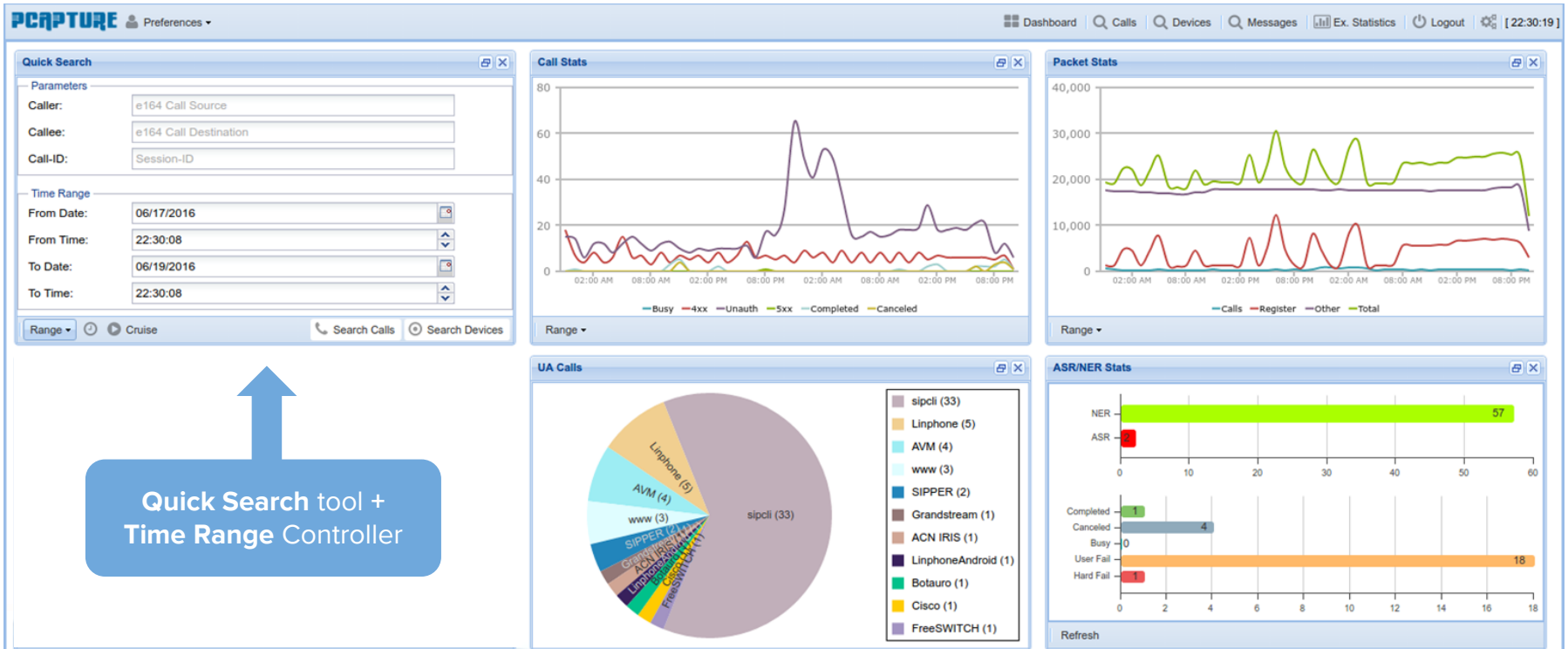
CaptAgent / RTPAgent

modular **capture agent**
supporting multiple
sockets, protocols and
transport methods

- **TZSP** support for MicroTik Packet Sniffer encapsulation
- **HEP** support for **HOMER** Cloud Analytics and Monitoring

```
{
  "CORRELATION_ID":"56a211936328-fgbtmubkimot",
  "RTP_SIP_CALL_ID":"56a211936328-fgbtmubkimot",
  "DELTA":19.980,
  "JITTER":0.023,
  "REPORT_TS":1453461919,
  "TL_BYTE":0,
  "SKEW":-0.180,
  "TOTAL_PK":510,
  "EXPECTED_PK":510,
  "PACKET_LOSS":0,
  "SEQ":0,
  "MAX_JITTER":1.892, "MEAN_JITTER":0.126,
  "MAX_DELTA":35.547, "MAX_SKEW":-15.615,
  "MIN_MOS":4.385, "MEAN_MOS":4.394, "MOS":4.394,
  "RFACOR":92.449, "MIN_RFACOR":92.013, "MEAN_RFACOR":92.444,
  "SRC_IP":"192.168.178.34", "SRC_PORT":58320,
  "DST_IP":"192.168.60.70", "DST_PORT":32728,
  "SRC_MAC":"00-04-13-29-64-22", "DST_MAC":"34-31-C4-38-24-0D",
  "CODEC_PT":9, "CLOCK":8000, "CODEC_NAME":"g722", "DIR":1,
  "REPORT_NAME": "192.168.178.34:58320", "PARTY":0,
  "TYPE":"PERIODIC"
}
```



Quick Search tool +
Time Range Controller

UI: Tracking Calls and Sessions in Real Time

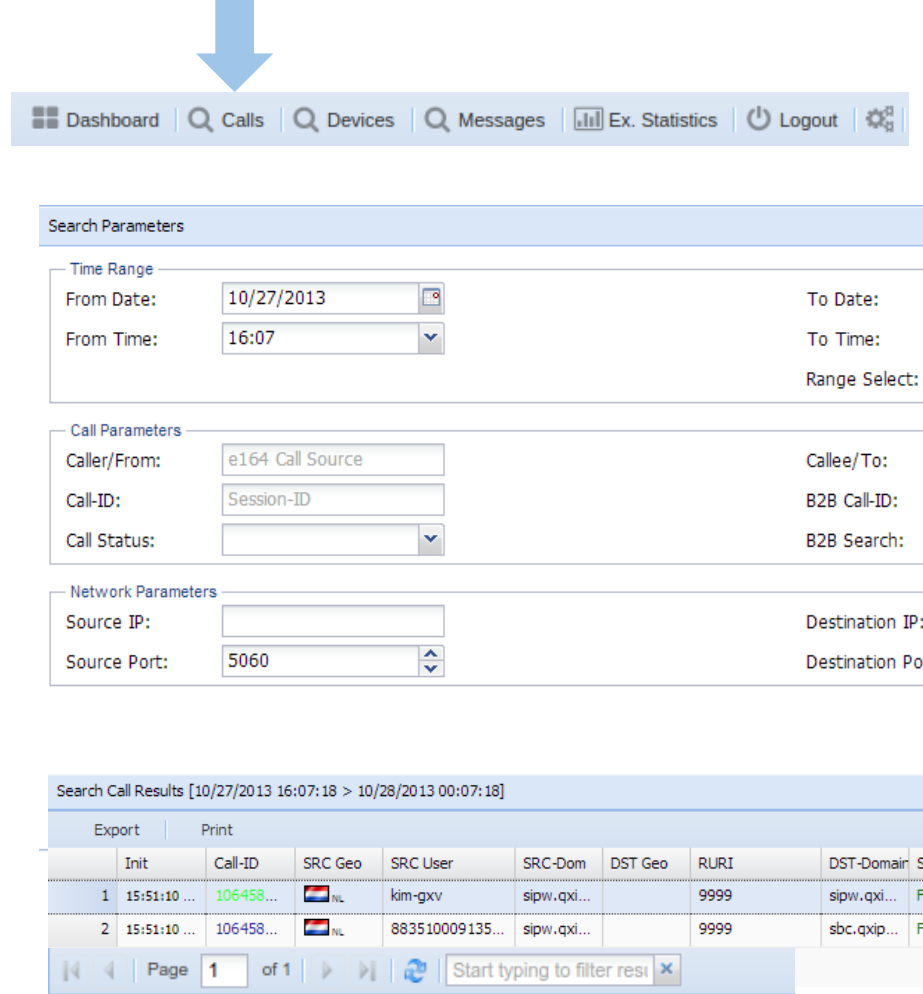
The **CALL SEARCH** functionality is one of the most used tools to locate, analyze and extract present and past call sessions.

The Call Search tool obeys the global **TIME-RANGE** as its primary filter, extended by a customizable number of user defined parameters targeting session headers and parameters (more in the next slide)

The **SEARCH** functionality also offers programmable “Search Profiles” per group used to automatically include and match multiple dialing patterns (*international/national*) prefixes (*00/+*) or routing prefixes from a bare number with no additional user interaction required.

To maximize the platform’s full potential, a “**two-tier**” approach is also possible and suggested, with a first initial group of results returned by the backend and complex filtering by any field can be performed client-side using advanced regex patterns and wildcard matching.

NEXT: TRACKING CALLS AND SESSIONS



The screenshot displays the Voicenter Call Search interface. At the top, a navigation bar includes links for Dashboard, Calls, Devices, Messages, Ex. Statistics, Logout, and a settings icon. A large blue arrow points down to the 'Calls' link. Below the navigation bar is the 'Search Parameters' section, which is divided into three main areas: Time Range, Call Parameters, and Network Parameters. The Time Range section includes fields for From Date (10/27/2013), To Date, From Time (16:07), To Time, and a Range Select dropdown. The Call Parameters section includes fields for Caller/From (e164 Call Source), Callee/To, Call-ID (Session-ID), B2B Call-ID, Call Status, and B2B Search. The Network Parameters section includes fields for Source IP, Destination IP, Source Port (5060), and Destination Port. Below the search parameters is the 'Search Call Results' section, which shows a table of results for the time range [10/27/2013 16:07:18 > 10/28/2013 00:07:18]. The table has columns for Init, Call-ID, SRC Geo, SRC User, SRC-Dom, DST Geo, RURI, and DST-Domain. Two results are shown, both with a duration of 15:51:10 and a Call-ID of 106458... The first result has SRC User 'kim-gxv' and SRC-Dom 'sipw.qxi...'. The second result has SRC User '883510009135...' and SRC-Dom 'sipw.qxi...'. Below the table is a pagination bar showing 'Page 1 of 1' and a search filter input field.

Dashboard | Calls | Devices | Messages | Ex. Statistics | Logout | Settings

Search Parameters

Time Range

From Date: 10/27/2013 To Date:

From Time: 16:07 To Time:

Range Select:

Call Parameters

Caller/From: e164 Call Source Callee/To:

Call-ID: Session-ID B2B Call-ID:

Call Status: B2B Search:

Network Parameters

Source IP: Destination IP:

Source Port: 5060 Destination Port:

Search Call Results [10/27/2013 16:07:18 > 10/28/2013 00:07:18]

	Init	Call-ID	SRC Geo	SRC User	SRC-Dom	DST Geo	RURI	DST-Domain
1	15:51:10 ...	106458...	NL	kim-gxv	sipw.qxi...		9999	sipw.qxi...
2	15:51:10 ...	106458...	NL	883510009135...	sipw.qxi...		9999	sbw.qxi...

Page 1 of 1

Start typing to filter results

UI: Tracking Calls and Sessions in Real Time

(continued)

Search Results for Calls will be returned in a table, ordered by timestamp and ready to use

PCAPTURE core is *session aware* and can display call status in realtime and aggregate all messages, statistics and logs in a single object, with automatic correlation to any other connected B2BUA legs

To investigate Session Details, just **click** on a result

Search Results table columns can be configured based on user preference to show or conceal any of the available session and protocol parameters.

Init	Call-ID	SRC Geo	SRC User	SRC-Dom	DST Geo	RURI
		Sort Ascending				
		Sort Descending				
		Columns	☒ Init			
		Filters	☐ Connect			
			☐ Disconnect			
			☒ Call-ID			
			☒ SRC Geo			
			☒ SRC User			
			☒ SRC-Dom			

	Init	Call-ID	User-Agent	SRC Geo	SRC User	DST User	RURI User	Status	Duration
1	21:30:28 201...	45525100-7...	Cisco-CUC...		fc305	9999	9999	Canceled	00:00:00
2	20:59:31 201...	F8C9FC28C...	AVM FRITZ...	RU	141	142	142	Canceled	00:00:00
3	21:34:03 201...	9f3ee11f-b0...	Botao ser...	DE	108	127	127	Canceled	00:00:00
4	20:59:51 201...	4132F63C8...	AVM FRITZ...	RU	141	142	142	Canceled	00:00:00
5	20:59:51 201...	d7a6b9df-b...	Botao ser...	DE	141	142	142	Canceled	00:00:00
6	21:34:03 201...	A40AE5BD...	AVM FRITZ...	DE	108	127	127	Canceled	00:00:00
7	20:57:57 201...	011FE30D8...	AVM FRITZ...	DE	142	141	141	Finished	00:01:05
8	21:00:16 201...	13EF9F81A...	AVM FRITZ...	RU	141	142	142	Finished	00:05:39
9	21:00:16 201...	e69ee634-b...	Botao ser...	DE	141	142	142	Finished	00:05:39
10	20:57:57 201...	940214d0-b...	Botao ser...	DE	142	141	141	Finished	00:01:05
11	21:27:58 201...	197283537...	Grandstrea...	NL	250	5000	5000	Finished	00:01:29
12	21:32:07 201...	609816358...	Grandstrea...	NL	gststream	9999	9999	Finished	00:01:36
13	21:22:25 201...	194615429...	Grandstrea...	NL	250	5000	5000	Finished	00:00:52
14	21:20:40 201...	ca25aaa942...	sipcli/v1.8	FR	107	00025546844682212	00025546844682212	4xx Failure	00:00:00
15	21:15:07 201...	f77d69ff19c...	sipcli/v1.8	FR	107	5118442038682803	5118442038682803	4xx Failure	00:00:00
16	21:14:00 201...	a3788a4f38...	sipcli/v1.8	FR	107	+41435085386	+41435085386	4xx Failure	00:00:00
17	21:12:05 201...	ad9e452b6...	sipcli/v1.8	FR	107	~810441277509067	~810441277509067	4xx Failure	00:00:00
18	20:40:49 201...	2a7d51762...	sipcli/v1.8	FR	107	66981046844682212	66981046844682212	4xx Failure	00:00:00
19	20:51:55 201...	c22293a288...	sipcli/v1.8	US	4010	00414441252759819	00414441252759819	Unauthori...	00:00:00
20	20:54:39 201...	d8ac648e5b...	sipcli/v1.8	US	1	0037052078511	0037052078511	Unauthori...	00:00:00
21	21:18:59 201...	7a78112bca...	sipcli/v1.8	GB	870	00441729810030	00441729810030	Unauthori...	00:00:00
22	21:33:45 201...	e591d0c08f...	sipcli/v1.8	GB	870	000441729810030	000441729810030	Unauthori...	00:00:00
23	21:09:40 201...	fec0394ee3...	sipcli/v1.8	GB	100002	000441224928143	000441224928143	Unauthori...	00:00:00
24	21:28:44 201...	c8ec5407c3...	sipcli/v1.8	US	4010	600441252759819	600441252759819	Unauthori...	00:00:00
25	20:44:42 201...	a650ad2a5...	sipcli/v1.8	GB	3003	002441252759842	002441252759842	Unauthori...	00:00:00
26	21:01:39 201...	b199dc478e...	sipcli/v1.8	GB	9031	00441372230055	00441372230055	Unauthori...	00:00:00
27	21:27:41 201...	8b4817e4b...	sipcli/v1.8	GB	9031	000441372230055	000441372230055	Unauthori...	00:00:00
28	21:10:20 201...	2e00b92aa...	sipcli/v1.8	US	4010	500441252759819	500441252759819	Unauthori...	00:00:00
29	21:23:33 201...	1486fa4d-b...	Botao ser...	DE	250	1234	1234	Initializing	00:00:00
30	21:23:02 201...	1486fa4d-b...	Botao ser...	DE	250	1234	1234	Initializing	00:00:00

UI: Tracking Calls and Sessions Details

(continued)

Session Details will be returned when selecting one or more result rows. The API will automatically fetch all correlated call data in the current Time Range.

The “Session Detail” window features several Tabs presenting available correlated information about the Session (or Session Group) being displayed.

Call Session tab presents packets in *Shark-View* mode

Each packet and message can be inspected in any display mode by simply clicking the corresponding row or object to reveal the full original payload data

Session: cea42fb5-af62-1234-21a5-0030487e5dc6

Call Session	Call Flow	Voice Quality	Geo Maps	Devices	Export	Logs
Timestamp	Diff	Bytes	Timestamp MS	SRC IP	SRC Port	DST IP
1 06/17/2016 21:16:17		1072	1466190977197327	225.128	61531	.65.77
2 06/17/2016 21:16:17		298	1466190977197914	.65.77	5060	.225.128
3 06/17/2016 21:16:17	=	664	1466190977219044	.65.77	5060	.225.128
4 06/17/2016 21:16:17	=	353	1466190977290431	.225.128	61531	.65.77
5 06/17/2016 21:16:17	=	1328	1466190977311900	.225.128	61531	.65.77
6 06/17/2016 21:16:17	=	298	1466190977312193	.65.77	5060	.225.128
7 06/17/2016 21:16:17	=	1029	1466190977333606	.65.77	5060	.100.120
8 06/17/2016 21:16:17	=	382	1466190977380994	.100.120	5060	.65.77
9 06/17/2016 21:16:17	=	474	1466190977493226	.100.120	5060	.65.77
10 06/17/2016 21:16:17	=	665	1466190977513901	.65.77	5060	.225.128
11 06/17/2016 21:16:38	+21...	995	1466190998411410	.100.120	5060	.65.77
12 06/17/2016 21:16:38	=	438	1466190998413634	.65.77	5060	.100.120
13 06/17/2016 21:16:38	=	1010	1466190998433718	.65.77	5060	.225.128
14 06/17/2016 21:16:38	=	463	1466190998531771	.225.128	61531	.65.77
15 06/17/2016 21:16:51	+13...	855	1466191011835062	.225.128	61531	.65.77
16 06/17/2016 21:16:51	=	439	1466191011864164	.65.77	5060	.225.128
17 06/17/2016 21:16:51	=	721	1466191011893650	.65.77	5060	.100.120
18 06/17/2016 21:16:51	=	711	1466191011940298	.100.120	5060	.65.77

UI: Tracking Calls and Sessions Details

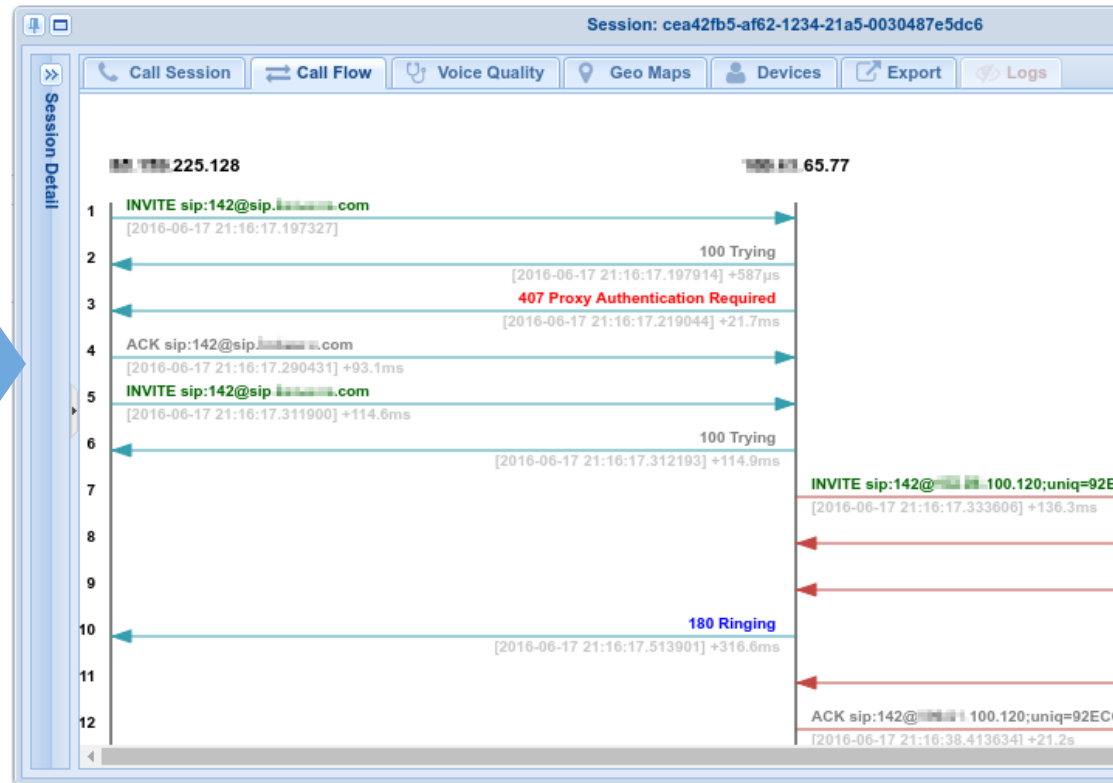
(continued)

Sessions involving several devices with hops traversing multiple systems can quickly get complex

PCAPTURE's *Call Flow* tool automatically correlates hosts and messages and presents them in an easy to interpret format well familiar to voice experts of all seasons and capable of handling unlimited legs

Call Flow tab presents packets in Signaling *Flow* mode

Each packet and message can be inspected in any display mode by simply clicking the corresponding row or object to reveal the full original payload data

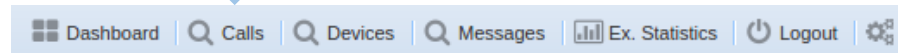


UI: Tracking Calls and Sessions Details

(continued)

When additional data about the Session being inspected is available, PCAPTURE will automatically present it to the end-user without any interaction.

The **Export Tab** provides dynamic methods to Save, Archive or Share the current set in different formats.



Voice Quality tab presents stream RTP-RTCP quality reports

Geo Maps tab presents the approx. IP Geolocation of User Agents

Devices tab presents details about *Registered* SIP User-Agents

Session: cea42fb5-af62-1234-21a5-0030487e5dc6

User-Agent QoS Reports

Call-ID	Reporter	Timestamp	RTP Source	RTP Destination	< Jitter	> Jitter	< L...	> L...	< Packets	> Packets	RT...	MOS	R-F...
cea42fb...	1:BYE	21:16:51	10.0.0.65.77	10.0.0.100.120	0	0	0	0	427	442	0	4.4...	93.2
cea42fb...	1:200	21:16:51	10.0.0.100.120	10.0.0.65.77	23	0	0	0	440	392	0	4.4...	93.2
37A8D1...	1:BYE	21:16:51	10.0.0.225.128	10.0.0.65.77	0	0	0	0	427	442	0	4.4...	93.2

nVoice QoS Reports

Call-ID	RTP Times...	RTP Source	RTP Destination	< Jitter	> Jitter	< L...	> L...	< Packets	> Packets	< Latency	> Latency	MOS	R-F...
---------	--------------	------------	-----------------	----------	----------	--------	--------	-----------	-----------	-----------	-----------	-----	--------

RTPAgent RTP QoS Reports

Timestamp	RTP Src	RTP Dst	Jitter	Los...	Tot. Pkts	Latency	Skew	MOS	Me...	R-F...	Type	Co...
-----------	---------	---------	--------	--------	-----------	---------	------	-----	-------	--------	------	-------

Session: cea42fb5-af62-1234-21a5-0030487e5dc6

Map

Session: cea42fb5-af62-1234-21a5-0030487e5dc6

Device Registrations

Time	User	Auth	Domain	IP	Port	Geo	UAS	Exp...	Sta...
21:00:49 2016...	141	141	sip.141.com	10.0.0.225.128	615...	RU	AVM FRITZ/Box Fon WLAN...	1800	3

UI: Tracking Media Session Quality

(continued)

The **Voice Quality** tab presents metrics related to media sessions as reported by User-Agents, Passive Network Probes and Media Control Protocols, providing correlated data useful when analyzing complex RTP media paths between SIP Endpoints

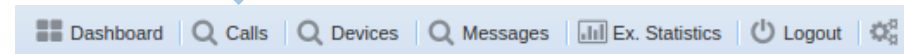
User-Agent generated media reports (*RTCP-XR, X-RTP-Stat, P-RTP*)

CAs can automatically report for monitored streams at variable or static rates, with each report carrying all RTP metrics and **MOS**

RTP Report from passive network analysis with granular metrics

CAs can also capture and aggregate RTCP control protocol messages and extract metrics and statistics to calculate a **MOS**

RTCP Report from analysis and aggregation of User-Agent reports



Session: 5767f278e767-zhqvpgu8and

Call Session | Call Flow | **Voice Quality** | Geo Maps | Devices | Export | Logs

User-Agent QoS Reports

Call-ID	Reporter	Timestamp	RTP Source	RTP Destination	< Jitter	> Jitter	< L...	> L...	<
5767f278e...	100-PUBL...	15:47:56	192.168.1.35.109	192.168.1.65.77	3	2	0	0	0
5767f278e...	4:200:	15:47:56	192.168.1.35.109	192.168.1.65.77	0	0	0	0	2
5767f278e...	4:200:	15:47:56	192.168.1.35.109	192.168.1.65.77	0	0	0	0	2

nVoice QoS Reports

Call-ID	RTP Timestamp	RTP Source	RTP Destination	< Jitter	> Jitter	< L...	> L...	< Packets	> Packets
---------	---------------	------------	-----------------	----------	----------	--------	--------	-----------	-----------

RTPAgent RTP QoS Reports

group: 109.69.65.77:20004

Timestamp	RTP Src	RTP Dst	InterArr. Jitter	Frac...	Tot. Pkts	SR Delay	Cum packet I
15:41:39 2016/06/20	192.168.1.65.77	192.168.1.157.55	0.019	0	1039	19.998	0.053
15:42:00 2016/06/20	192.168.1.65.77	192.168.1.157.55	0.018	0	1049	19.994	-20.002
15:42:21 2016/06/20	192.168.1.65.77	192.168.1.157.55	0.025	0	1051	20.011	-0.015
15:42:42 2016/06/20	192.168.1.65.77	192.168.1.157.55	0.017	0	1051	19.994	0.009
15:43:03 2016/06/20	192.168.1.65.77	192.168.1.157.55	0.019	0	1051	19.984	0.012
15:43:24 2016/06/20	192.168.1.65.77	192.168.1.157.55	0.018	0	1051	19.991	-0.003
15:43:45 2016/06/20	192.168.1.65.77	192.168.1.157.55	0.02	0	1051	20.011	-0.012
15:44:06 2016/06/20	192.168.1.65.77	192.168.1.157.55	0.028	0	1051	20.01	0.007
15:44:27 2016/06/20	192.168.1.65.77	192.168.1.157.55	0.022	0	1051	19.999	0.012
15:44:48 2016/06/20	192.168.1.65.77	192.168.1.157.55	0.019	0	1042	20.002	19.987

RTPAgent RTCP QoS Reports

group: 92.204.35.109:53505

Timestamp	RTP Src	RTP Dst	InterArr. Jitter	Frac...	Tot. Pkts	SR Delay	Cum packet I
15:41:36 2016/06/20	192.168.1.35.109	192.168.1.65.77	0.855	0	1011	20.168	-0.694
15:41:57 2016/06/20	192.168.1.35.109	192.168.1.65.77	1.292	0	1051	19.677	-0.337
15:42:18 2016/06/20	192.168.1.35.109	192.168.1.65.77	0.457	0	1051	20.117	-0.963
15:42:39 2016/06/20	192.168.1.35.109	192.168.1.65.77	0.344	0	1051	19.867	0.329
15:43:00 2016/06/20	192.168.1.35.109	192.168.1.65.77	0.278	0	1051	19.773	-0.441
15:43:21 2016/06/20	192.168.1.35.109	192.168.1.65.77	0.295	0	1051	20.468	-0.717
15:43:42 2016/06/20	192.168.1.35.109	192.168.1.65.77	0.276	0	1051	19.471	0.417
15:44:03 2016/06/20	192.168.1.35.109	192.168.1.65.77	0.471	0	1051	21.92	-2.221

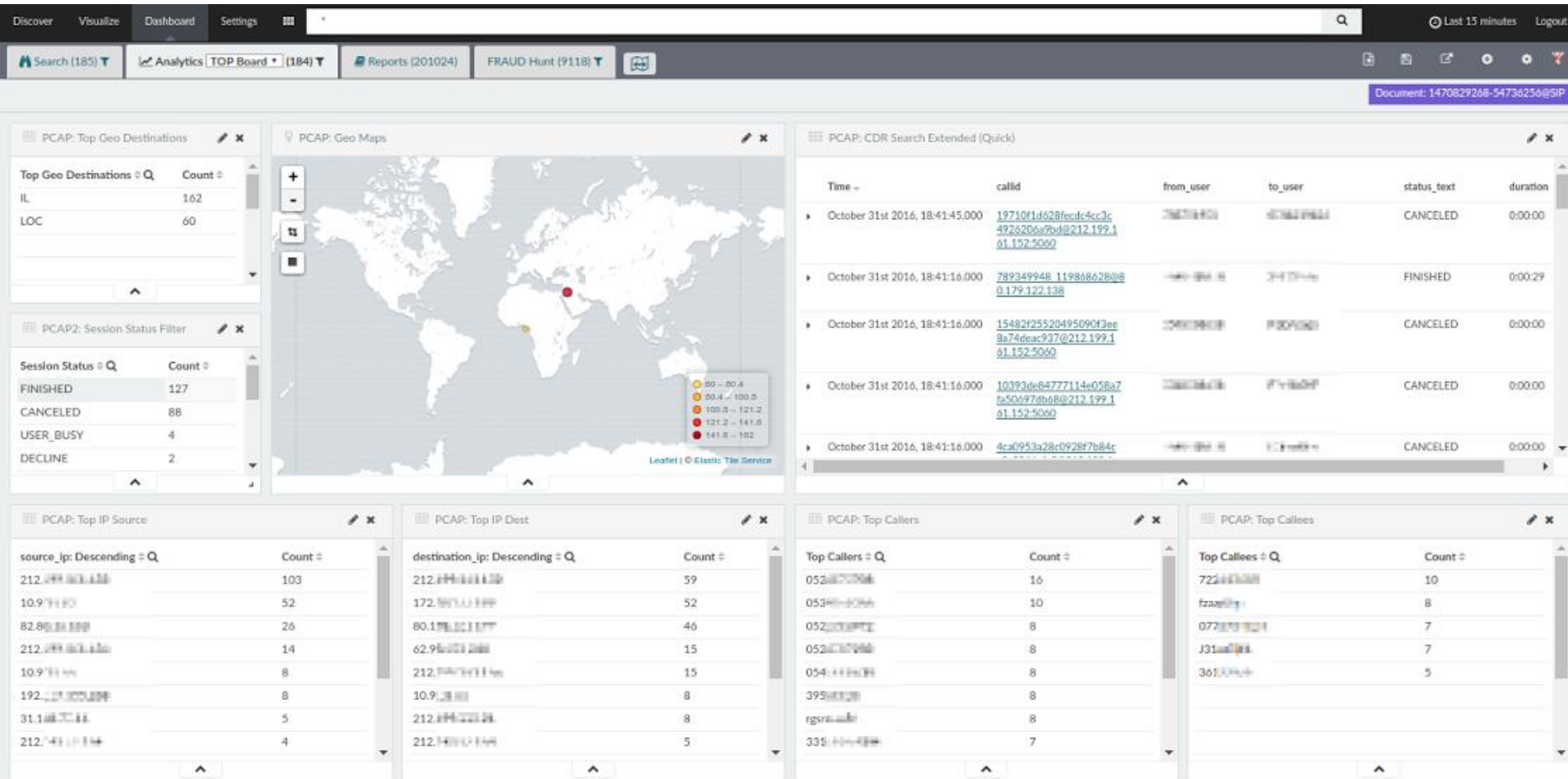
UI: Tracking Registrations and Devices

PCAPTURE features a dedicated tool for *Searching* and *Filtering* registration with *Expiration tracking*, integrated with Call Search tools:

Init	Call-ID	UAC	SRC Geo	User	Auth	Domain	Status	Expiration	Proto	SRC IP	SP...	DST IP	DP...
22:30:45 2016-06-19	1292262599...	ACN IRIS X ...		145	145	sip.145.145.com	Registered	Expired	SIP/UDP	145.145.145.36.186	407...	145.145.145.65.77	5060
22:30:52 2016-06-19	219111350-...	Grandstream...		lab	lab	sip.lab.145.com	Registered	Expired	SIP/UDP	145.145.145.44.127	5062	145.145.145.6.157.55	5060
22:31:23 2016-06-19	57EF618711...	AVM FRITZ!		141	141	sip.141.141.com	Registered	00:08:12	SIP/UDP	141.141.141.225.128	615...	141.141.141.65.77	5060
22:32:32 2016-06-19	386d439b1b...	snom360/8...		123456789_pc	123456789_pc	sip.123456789_pc.145.com	Registered	Expired	SIP/UDP	123456789_pc.20.17	2048	123456789_pc.65.77	5060
22:33:43 2016-06-19	491551672-...	ACN IRIS X ...		147	147	sip.147.147.com	Registered	Expired	SIP/UDP	147.147.147.161.3	187...	147.147.147.65.77	5060
22:35:02 2016-06-19	386d439b1b...	snom360/8...		123456789_pc	123456789_pc	sip.123456789_pc.145.com	Registered	Expired	SIP/UDP	123456789_pc.20.17	2048	123456789_pc.65.77	5060
22:35:27 2016-06-19	818978511-...	ACN IRIS X ...		204	204	sip.204.204.com	Registered	Expired	SIP/UDP	204.204.204.100.120	114...	204.204.204.65.77	5060
22:35:37 2016-06-19	918051609-...	Grandstream...		gstream	gstream	sip.gstream.145.com	Registered	-	SIP/UDP	gstream.44.127	550...	gstream.6.157.55	5060
22:35:54 2016-06-19	219111350-...	Grandstream...		lab	lab	sip.lab.145.com	Registered	Expired	SIP/UDP	lab.44.127	5062	lab.6.157.55	5060
22:37:33 2016-06-19	386d439b1b...	snom360/8...		123456789_pc	123456789_pc	sip.123456789_pc.145.com	Registered	Expired	SIP/UDP	123456789_pc.20.17	2048	123456789_pc.65.77	5060
22:38:15 2016-06-19	1292262599...	ACN IRIS X ...		145	145	sip.145.145.com	Registered	00:00:03	SIP/UDP	145.145.145.36.186			
22:38:40 2016-06-19	3024034456...	S450 IP/022...		101	101	sip.101.101.com	Registered	Expired	SIP/UDP	101.101.101.36.186			
22:39:54 2016-06-19	AC6A5EE4E...	AVM FRITZ!		139	139	sip.139.139.com	Registered	00:16:42	SIP/UDP	139.139.139.1.19			
22:40:03 2016-06-19	2086355230...	Grandstream...		lab	lab	sip.lab.145.com	Registered	Expired	SIP/UDP	lab.44.127			
22:40:03 2016-06-19	386d439b1b...	snom360/8...		123456789_pc	123456789_pc	sip.123456789_pc.145.com	Registered	Expired	SIP/UDP	123456789_pc.20.17			
22:40:06 2016-06-19	1533980629...	Grandstream...		gstream	gstream	sip.gstream.145.com	Registered	-	SIP/UDP	gstream.44.127			
22:40:37 2016-06-19	918051609-...	Grandstream...		gstream	gstream	sip.gstream.145.com	Registered	-	SIP/UDP	gstream.44.127			
22:40:56 2016-06-19	219111350-...	Grandstream...		lab	lab	sip.lab.145.com	Registered	Expired	SIP/UDP	lab.44.127			
22:41:12 2016-06-19	491551672-...	ACN IRIS X ...		147	147	sip.147.147.com	Registered	00:03:00	SIP/UDP	147.147.147.161.3			
22:42:33 2016-06-19	386d439b1b...	snom360/8...		123456789_pc	123456789_pc	sip.123456789_pc.145.com	Registered	Expired	SIP/UDP	123456789_pc.20.17			
22:42:57 2016-06-19	818978511-...	ACN IRIS X ...		204	204	sip.204.204.com	Registered	00:04:45	SIP/UDP	204.204.204.100.120			
22:45:03 2016-06-19	386d439b1b...	snom360/8...		123456789_pc	123456789_pc	sip.123456789_pc.145.com	Registered	Expired	SIP/UDP	123456789_pc.20.17			
22:45:37 2016-06-19	918051609-...	Grandstream...		gstream	gstream	sip.gstream.145.com	Registered	-	SIP/UDP	gstream.44.127			

Call Session		Call Flow	
Timestamp	Diff		
1 06/17/2016 21:16:17			
2 06/17/2016 21:16:17			
3 06/17/2016 21:16:17	=		
4 06/17/2016 21:16:17	=		
5 06/17/2016 21:16:17	=		
6 06/17/2016 21:16:17	=		
7 06/17/2016 21:16:17	=		
8 06/17/2016 21:16:17	=		
9 06/17/2016 21:16:17	=		
10 06/17/2016 21:16:17	=		
11 06/17/2016 21:16:38	+21...		
12 06/17/2016 21:16:38	=		
13 06/17/2016 21:16:38	=		
14 06/17/2016 21:16:38	=		
15 06/17/2016 21:16:51	+13...		
16 06/17/2016 21:16:51	=		
17 06/17/2016 21:16:51	=		
18 06/17/2016 21:16:51	=		

Voice - Top Board



SESSION/PROTOCOL DRILLDOWN:

Discover
Visualize
Dashboard
Settings

Search (237)
Analytics (237)
Reports (200468)
FRAUD Hunt (9251)

uid: *6bb21660-9f90-11e6-9660-000019432987
Actions

Document: 1470829268-54736256@SIP

SHARKVIEW test
Shark-View
Call-Flow
Export

```

sequenceDiagram
    participant A as 10.18.18.55
    participant B as 10.177.203.5060
    A->>B: INVITE
    B-->A: 100
    A->>B: 180
    B->>A: 200
    A-->B: ACK
    B->>A: BYE
    A->>B: 200
    
```

Message: SIP/2.0 100 Trying

Via: SIP/2.0/UDP
10.18.18.55;branch=z9hG4bK4ed2.c598073.0;received=10.9.18.55

Via: SIP/2.0/UDP
172.18.177.203:5060;rport=5060;branch=z9hG4bKsj1vm102o8hcl86a4c1.1

ACK

Record-Route: <sip:10.9.18.55;lr=on;nat=yes>

From: <sip:0544687934@172.18.177.28>

To: <sip:0776704024@172.18.177.28>

Call-ID: 1470829268-54736256@SIP

CSeq: 1 INVITE

Server: Asterisk PBX certified/13.1-cert4

Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE

Supported: replaces, timer

Session-Expires: 1800;refresher=uas

Contact: <sip:0776704024@172.18.177.28>

Content-Length: 0

PCAP2: Avg. MOS Metric
4
Avg. MOS

PCAP2: Session Duration (total)
0:00:02
Duration (seconds)

PCAP: Call Flows (A/B)
7934
4024
0776704024

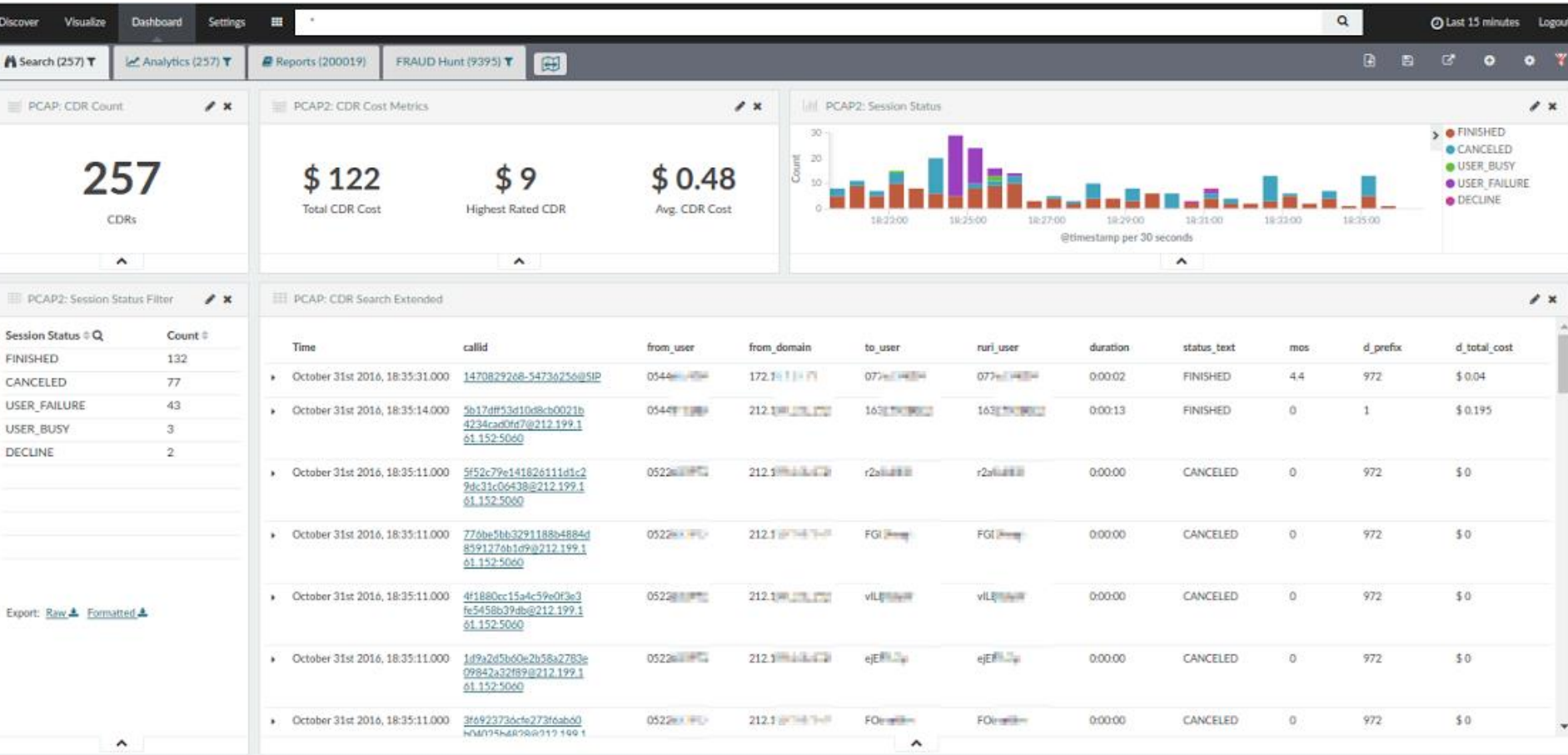
PCAP: Geo Maps
PCAP2: Codec In/Out

PCAP2: Cost Lookup
Prices - Hide (1)
cc description prefix price call cost
IL Programmable Outbound Minute - Israel 972 0.02000 0.0006666666666666666

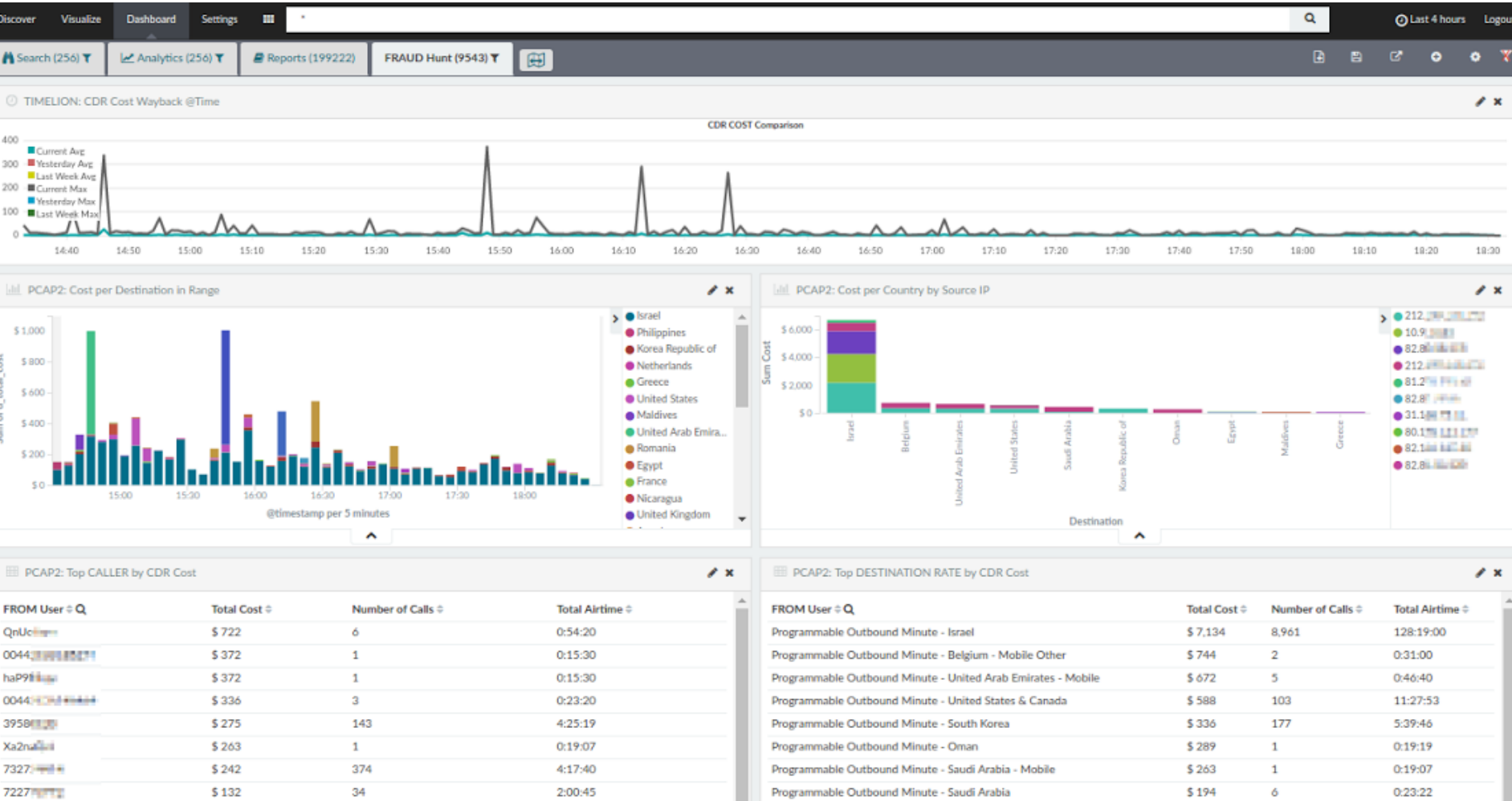
PCAP: CDR Search Extended (Quick)

Time	callid	from_user	to_user	status_text	duration
October 31st 2016, 18:35:31.000	1470829268-54736256@SIP	0544687934	0776704024	FINISHED	0:00:02

CDR SEARCH & FILTER:



FRAUD DETECTION PATTERNS:



Alerting and Fraud detection

SA: Time Series Visualization in Kibana

Complex reports can be created leveraging all available metrics and time series, including comparisons across different data ranges:

