



Na minha humilde opinião, quando alguém trabalha com servidores de comunicações, todos os recursos utilizados para facilitar seu trabalho é importante para as tarefas ao qual a pessoa se dedica a fazer. Por este motivo, um servidor dedicado, de Asterisk ou Kamailio, é uma prática comum instalar um ambiente gráfico.

Devido a isso, eu sempre fui um grande fã de ferramentas em modo texto, aqueles que, apesar de "simular" um ambiente gráfico, janelas e usarem cores básicas ou não, corre totalmente em modo texto, usando as teclas "especiais" como teclas de função ou teclas de setas para mover entre as opções. Não sobrecarregue o sistema, não ocupam recursos e sua funcionalidade é semelhante às ferramentas gráficas, mas muito mais eficaz do ponto de vista "tempo / recursos", além da necessidade de não precisar lutar com o mouse. Aplicativos como o Midnight Commander (versão Linux do Norton Commander) para o gerenciamento do sistema de arquivos, ou mesmo a ferramenta típica "memtest86" para verificar a memória RAM são alguns exemplos de ferramentas que funcionam em modo semi-gráfico usando a biblioteca "ncurses" e permitindo que ele seja muito prático, mas não menos atraente.

Concentrando-se em ToIP, GoIP TDMoIP e VoIP, com certeza, todos nós sabemos de uma ferramenta muito famosa chamada "Wireshark" uma ferramenta gráfica utilizada para capturar o tráfego de rede e ver confortavelmente no seu ambiente gráfico para analisar traços de comunicação. Semelhante a este, mas sem ambiente gráfico (para que possamos correr no mesmo sistema dedicado), existem outras ferramentas essenciais: **tshark** (wireshark versão ncurses) **ngrep** (outra ferramenta de captura e exibição de dados em pacotes. Este por sua vez amplamente utilizado em todo o ambiente ToIP, GoIP, TDMoIP e VoIP para analisar o protocolo SIP), com certeza também conhece o bom e velho **tcpdump**, (uma das primeiras ferramentas para capturar, filtrar e visualizar dados e conexões de traços), no entanto, acabei de encontrar uma grande ferramenta que passo apresentar e certamente passou a fazer parte da minha lista pessoal de ferramentas essenciais para os sistemas ToIP, GoIP, TDMoIP e VoIP.

Ivan Alonso [aka Kaian] <kaian@irontec.com> da IRONTEC nos presenteou com seu novo projeto o “**SNGREP**”, uma ferramenta semelhante ao **ngrep** (na verdade, é baseado nele), mas usa **ncurses** para exibir o fluxo SIP em modo texto, na console, algo que certamente é muito bom para muitos de nós em nosso dia a dia.

Sim, eu sei que existem muitas outras ferramentas que fazem o mesmo, **Homer SIP Captura**, por exemplo, mas eu gostei **SNGREP** considerando mais que:

- É muito fácil de compilar e instalar
- Ele quase não tem dependências, o que necessita provavelmente você já tem instalado.
- Ele não consome recursos (importantes em qualquer instrumento de medição)
- Rápido para instalar e executar (não defina mil coisas)
- Software livre

Por isso, encorajo-vos a experimentar, no seu servidor Asterisk e fazer os testes, você vai ter o comportamento do protocolo SIP para melhorar suas habilidades.

Tão simples de baixar, compilar e executar:

```
# cd /usr/local/src/sngrep
# aptitude install git
# git clone https://github.com/irontec/sngrep
# aptitude install libncurses5
# aptitude install ngrep
# aptitude install stdbuf
# apt-get install libpcap-dev
./Configure && make && make install
```

Comandos Basicos

Sngrep pode ser usado para visualizar os pacotes SIP de um arquivo pcap

```
# sngrep file.pcap
```

Ou on-line com o ngrep análise, usando filtros e parâmetros (man ngrep para uma lista completa de comandos)

```
# sngrep -O file.pcap port 5060 and udp and host 192.168.8.101
```

Se você compilou sem ngrep apoio, use somente os filtros.

```
# sngrep port 5060 and udp
```

Eu particularmente gostei de usar o ultimo comando veja as telas:

sngrep - SIP message interface for ngrep					
Current Mode: OffLine					
Filename: /tmp/largo.pcap					
From SIP	To SIP	Msg	From	To	Starting
farsa@127.0.0.1:34898	test@127.0.0.1:5060	2	127.0.0.1:34898	127.0.0.1:5060	OPTIONS
asterisk@10.10.9.40	10.10.0.11	2	10.10.9.40:5060	10.10.0.11:5060	OPTIONS
24014@10.10.9.40	194.30.0.111	2	10.10.9.40:5060	194.30.0.111:5060	OPTIONS
pbk@10.10.9.40	944625083@10.10.9.40	7	10.10.1.142:5063	10.10.9.40:5060	INVITE
24014@nommos.lva11d	944625083@194.30.0.111	3	10.10.9.40:5060	194.30.0.111:5060	INVITE
pbk@10.10.9.40	3998@10.10.9.40	11	10.10.1.142:5063	10.10.9.40:5060	INVITE
3998@10.10.9.40	pbk@10.10.1.142:5063	7	10.10.9.40:5060	10.10.1.142:5063	INVITE
pbk@10.10.9.40	3998@10.10.9.40	11	10.10.1.142:5063	10.10.9.40:5060	INVITE
3998@10.10.9.40	pbk@10.10.1.142:5063	7	10.10.9.40:5060	10.10.1.142:5063	INVITE
pbk@10.10.9.40	3998@10.10.9.40	10	10.10.1.142:5063	10.10.9.40:5060	INVITE
3998@10.10.9.40	pbk@10.10.1.142:5063	7	10.10.9.40:5060	10.10.1.142:5063	INVITE
pbk@10.10.9.40	3998@10.10.9.40	10	10.10.1.142:5063	10.10.9.40:5060	INVITE
pbk@10.10.9.40	3998@10.10.9.40	9	10.10.1.142:5063	10.10.9.40:5060	INVITE
3998@10.10.9.40	pbk@10.10.1.142:5063	7	10.10.9.40:5060	10.10.1.142:5063	INVITE
pbk@10.10.9.40	3998@10.10.9.40	10	10.10.1.142:5063	10.10.9.40:5060	INVITE
pbk@10.10.9.40	3998@10.10.9.40	14	10.10.1.142:5063	10.10.9.40:5060	INVITE
3998@10.10.9.40	pbk@10.10.1.142:5063	8	10.10.9.40:5060	10.10.1.142:5063	INVITE
pbk@10.10.9.40	3998@10.10.9.40	10	10.10.1.142:5063	10.10.9.40:5060	INVITE
3998@10.10.9.40	pbk@10.10.1.142:5063	7	10.10.9.40:5060	10.10.1.142:5063	INVITE
pbk@10.10.9.40	3998@10.10.9.40	19	10.10.1.142:5063	10.10.9.40:5060	INVITE
3998@10.10.9.40	pbk@10.10.1.142:5063	5	10.10.9.40:5060	10.10.1.142:5063	INVITE
pbk@10.10.9.40	3998@10.10.9.40	9	10.10.1.142:5063	10.10.9.40:5060	INVITE

Call Details for 7265473a-ab7c47b7

Call Flow		
10.10.1.142:5063	10.10.9.40:5060	
19:29:09.430085	INVITE	INVITE sip:3998@10.10.9.40 SIP/2.0
19:29:09.430427	INVITE	Via: SIP/2.0/UDP 10.10.1.142:5063;branch=2SHGbk-esfdadd
19:29:09.431177	401 Unauthorized	From: "pbkkaian" <sip:pbkkaian@10.10.9.40>;tag=01a75e1a1be303
19:29:09.444562	ACK	To: "Kalian Irontec" <sip:3998@10.10.9.40>
19:29:09.449368	INVITE	Call-ID: 7265473a-ab7c47b7@10.10.1.142
19:29:09.452659	100 Trying	CSeq: 101 INVITE
19:29:09.773836	CANCEL	Max-Forwards: 70
19:29:09.774583	487 Request Terminated	Contact: "pbkkaian" <sip:pbkkaian@10.10.1.142:5063>
19:29:09.774695	200 OK	Expires: 240
19:29:09.865593	ACK	User-Agent: Cisco/SPA504G-7.5.2b
		Content-Length: 397
		Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
		Supported: replaces
		Content-Type: application/sdp
		v=0
		o=- 51594026 51594026 IN IP4 10.10.1.142
		s=
		c=IN IP4 10.10.1.142
		t=0
		m=audio 16422 RTP/AVP 0 2 8 9 18 96 97 98 101
		a=rtpmap:0 PCMU/8000
		a=rtpmap:2 G726-32/8000
		a=rtpmap:6 PCMA/8000
		a=rtpmap:9 G722/8000
		a=rtpmap:18 G729a/8000
		a=rtpmap:96 G726-40/8000
		a=rtpmap:97 G726-24/8000
		a=rtpmap:98 G726-16/8000
		a=rtpmap:101 telephone-event/8000
		a=ftsp:101 0-15
		a=ptime:30
		a=sendrcv

Q: Quit C: Toggle color F: Show raw messages X: Show Extended Call-Flow

Call Details for 7265473a-ab7c47b7

Call Flow Extended			
10.10.1.142:5063	10.10.9.40:5060	10.10.1.142:5063	
19:29:09.430085	INVITE		INVITE sip:3998@10.10.9.40 SIP/2.0
19:29:09.430427	INVITE		Via: SIP/2.0/UDP 10.10.1.142:5063;branch=2SHGbk-esfdadd
19:29:09.431177	401 Unauthorized		From: "pbkkaian" <sip:pbkkaian@10.10.9.40>;tag=01a75e1a1be303
19:29:09.444562	ACK		To: "Kalian Irontec" <sip:3998@10.10.9.40>
19:29:09.449368	INVITE		Call-ID: 7265473a-ab7c47b7@10.10.1.142
19:29:09.452659	100 Trying		CSeq: 101 INVITE
19:29:09.756403		INVITE	Max-Forwards: 70
19:29:09.773836	CANCEL		Contact: "pbkkaian" <sip:pbkkaian@10.10.1.142:5063>
19:29:09.774583	487 Request Terminated		Expires: 240
19:29:09.774695	200 OK		User-Agent: Cisco/SPA504G-7.5.2b
19:29:09.781957	200 OK	100 Trying	Content-Length: 397
19:29:09.782465		CANCEL	Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
19:29:09.865593	ACK		Supported: replaces
19:29:09.877126		180 Ringing	Content-Type: application/sdp
19:29:09.883097		487 Request Terminated	v=0
19:29:09.883543		ACK	o=- 51594026 51594026 IN IP4 10.10.1.142
19:29:09.884717		200 OK	s=
			c=IN IP4 10.10.1.142
			t=0
			m=audio 16422 RTP/AVP 0 2 8 9 18 96 97 98 101
			a=rtpmap:0 PCMU/8000
			a=rtpmap:2 G726-32/8000
			a=rtpmap:6 PCMA/8000
			a=rtpmap:9 G722/8000
			a=rtpmap:18 G729a/8000
			a=rtpmap:96 G726-40/8000
			a=rtpmap:97 G726-24/8000
			a=rtpmap:98 G726-16/8000
			a=rtpmap:101 telephone-event/8000
			a=ftsp:101 0-15
			a=ptime:30
			a=sendrcv

Q: Quit C: Toggle color F: Show raw messages X: Show Call-Flow

Uma ótima ferramenta! Parabéns ao [Ivan](#) e a [IRONTEC](#) não somente por desenvolver, mas pelo fato de disponibilizar esta excelente ferramenta para a comunidade.