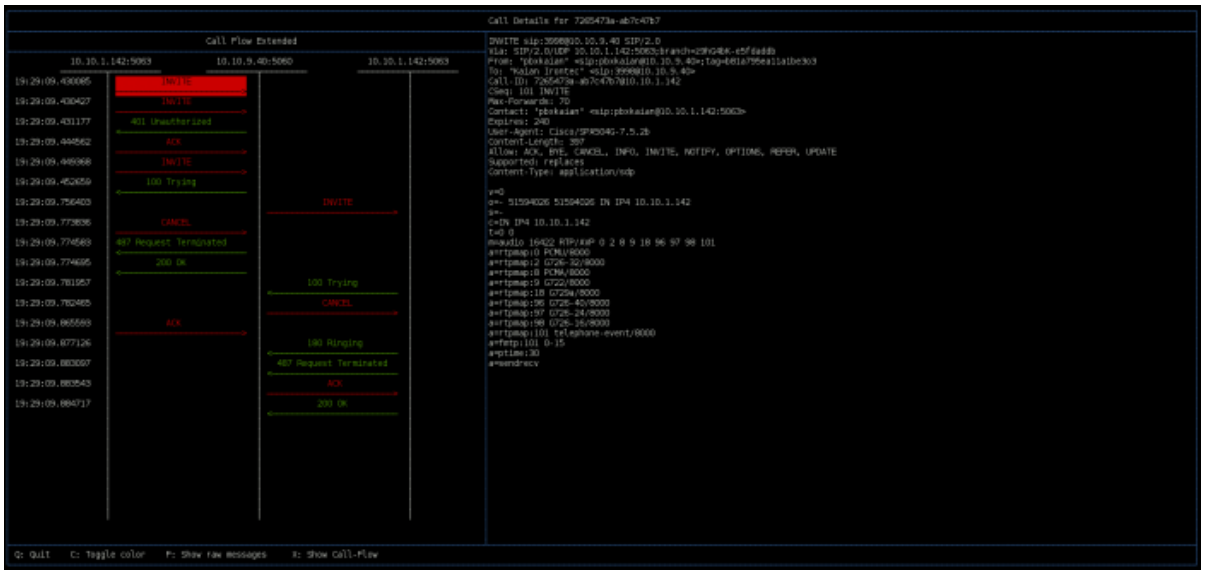
Na minha humilde opinião, quando alguém trabalha com servidores de comunicações, todos os recursos utilizados para facilitar seu trabalho é importante para as tarefas ao qual a pessoa se dedica a fazer. Por este motivo, um servidor dedicado, de Asterisk ou Kamailio, é uma prática comum instalar um ambiente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

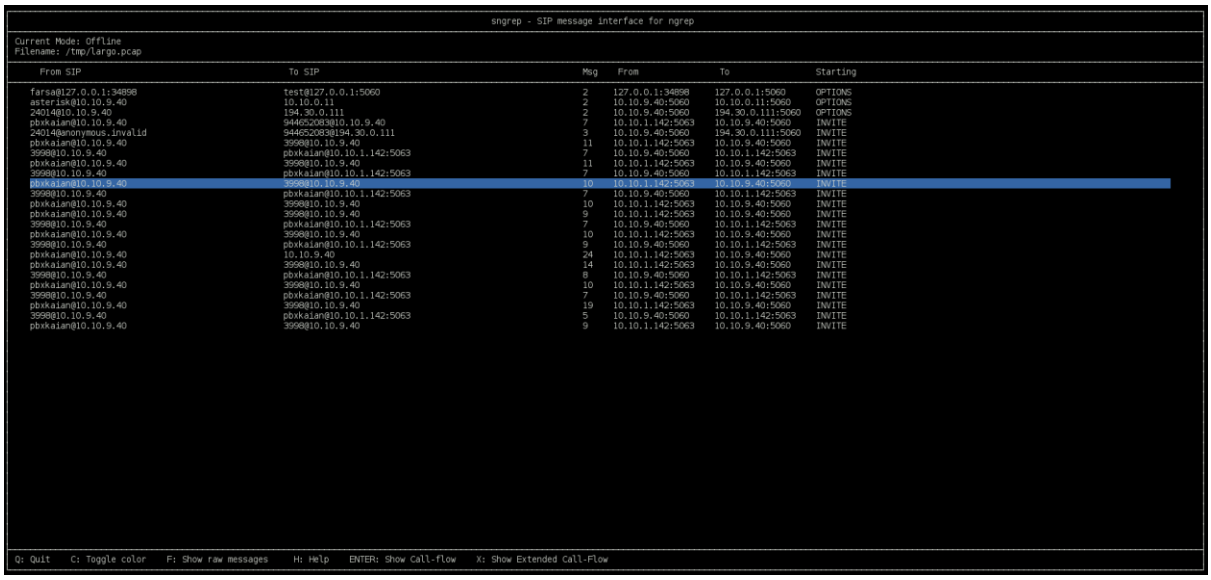
Ou on-line com o ngrep análise, usando filtros e parâmetros (man ngrep para uma lista completa de comandos)

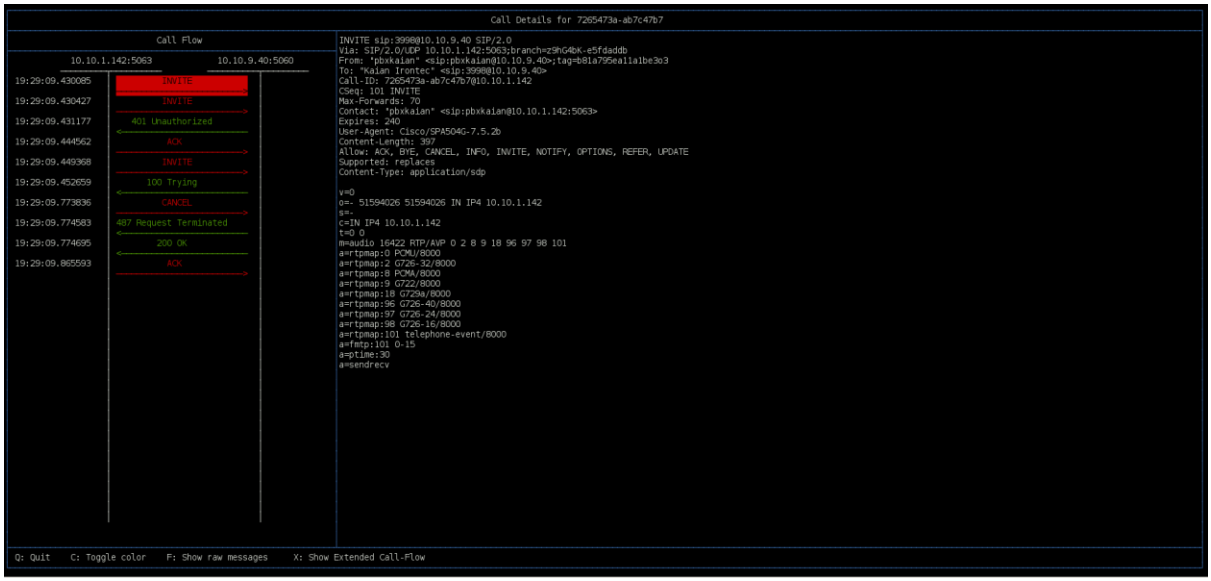
sngrep -O file.pcap port 5060 and udp and host 192.168.8.101

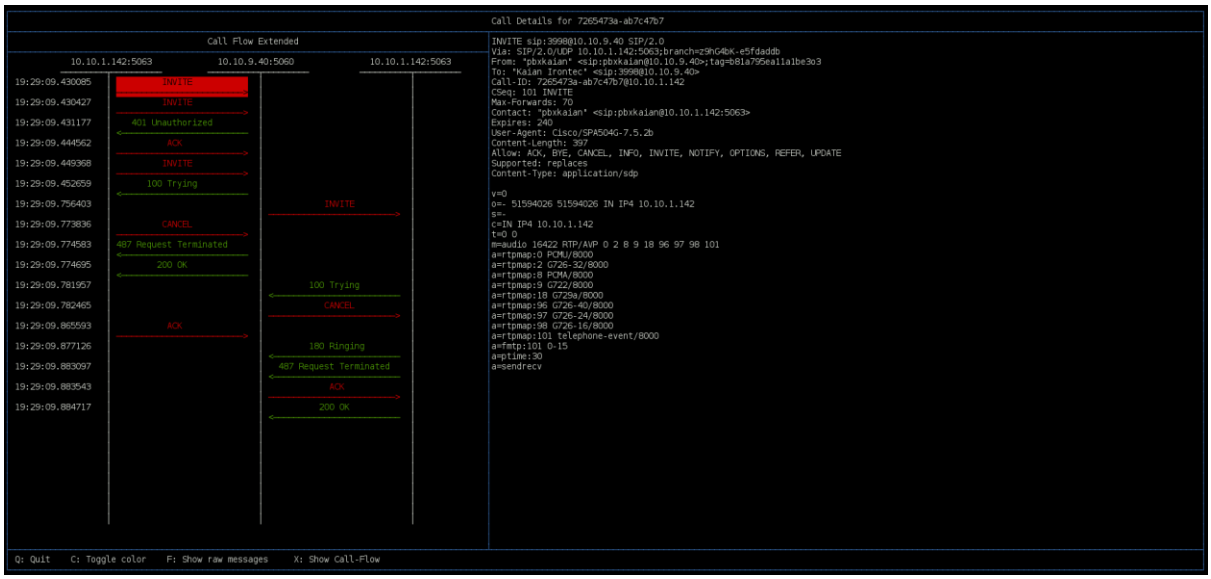
Se você compilou sem ngrep apoio, use somente os filtros.

sngrep port 5060 and udp

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







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