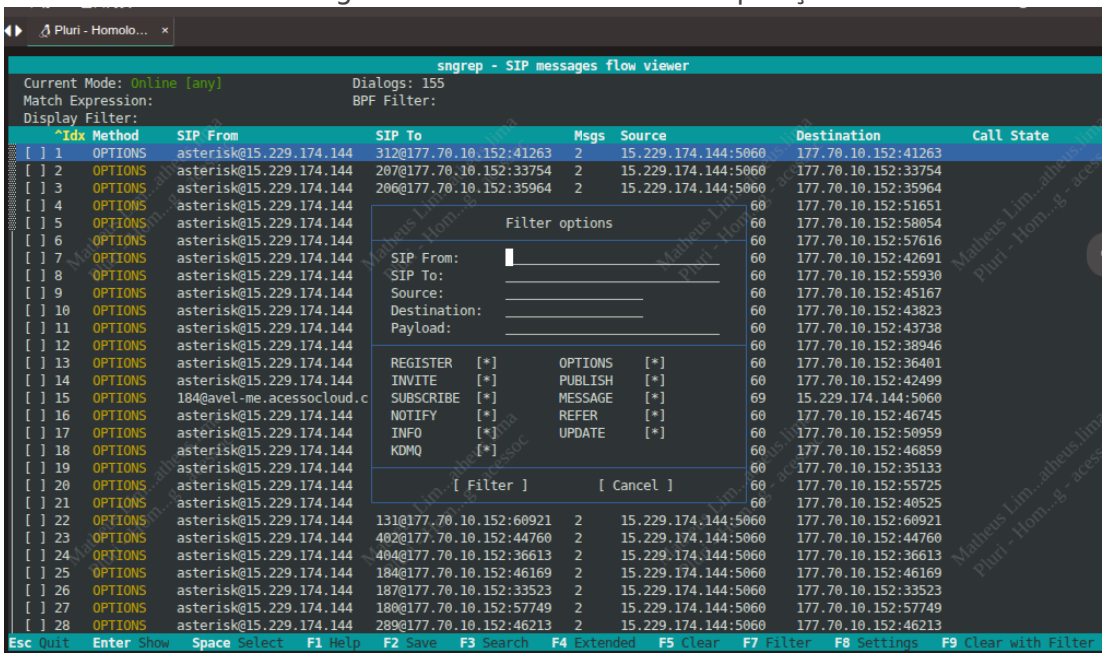
SNGREP

Using SNGREP

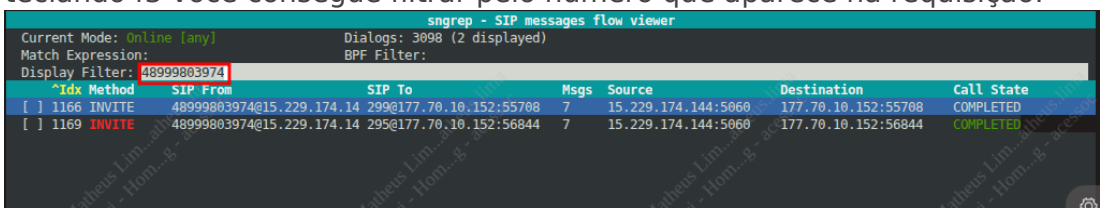
Consultar chamadas SIP:

-> `sngrep`

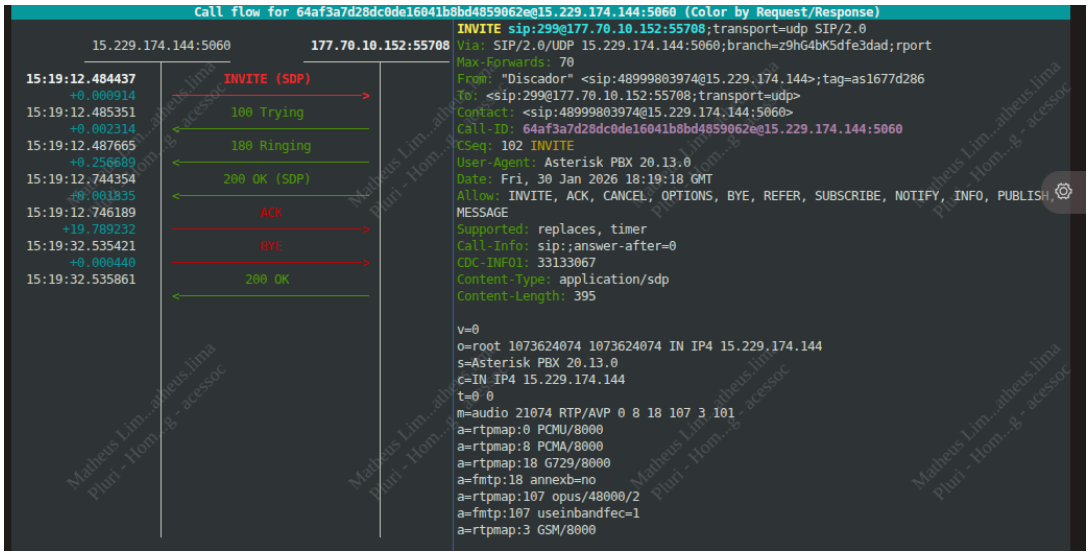
- Teclando f7 você consegue filtrar os métodos de requisição SIP



- teclando f3 você consegue filtrar pelo número que aparece na requisição:



- Ex de ligação no sngrep:



- **INVITE:** Indica que o usuário está sendo convidado a participar de uma sessão multimídia.
- **Trying:** Indica que a requisição está sendo processada.
- **200 OK(Answer):** Indica a confirmação de atendimento.
- **ACK:** Confirmação de mensagem recebida como resposta final a um INVITE.
- **OPTIONS:** Faz uma pergunta sobre quais métodos e extensões são suportados pelo servidor e pelo usuário descrito no campo de cabeçalho.
- **BYE: Usado para liberar os recursos associados a uma ligação e forçar a desconexão/desligamento da mesma.**
- **CANCEL: Cancela uma requisição que ainda esteja pendente, ou seja, em andamento.**

Main Screen

- ◦ **Idx**: Coluna do **número da linha**.
  ◦ **Method**: Coluna do **tipo de mensagem SIP**.
  ◦ **SIP From**: Coluna do **campo "De" (From) da mensagem SIP**.
  ◦ **SIP To**: Coluna do **campo "Para" (To) da mensagem SIP**.
  ◦ **Msgs**: Coluna da **quantidade numérica de mensagens**.
  ◦ **Source**: Coluna do **IP e porta de origem**.
  ◦ **Destination**: Coluna do **IP e porta de destino**.
  ◦ **Call State**: Coluna do **identificador da chamada**.

  image
- ◦ **ESC Quit**: Pressione **ESC** para sair do **sngrep**.
  ◦ **Enter**: Mostra **mais informações** sobre a linha destacada.
  ◦ **Space**: Ao pressionar **barra de espaço**, a linha é **selecionada**. Isso permite selecionar **múltiplas linhas** e pode ser usado junto com a opção **F2 (salvar)**.
  ◦ **F1 Help**: Abre o **menu de ajuda**.

- **F2 Save**: Permite **salvar a sessão atual de captura** (diálogos) em um arquivo **.pcap ou .txt**, definindo **caminho e nome do arquivo**.
- **F3 Search**: Permite **pesquisar** de forma **mais específica e detalhada**.
- **F4 Extended**: Mostra uma **visualização estendida**.
- **F5 Clear**: **Limpa a tela**.
- **F7 Filter**: Similar à busca, mas com **mais opções de filtro** para refinar os resultados.
- **F8 Settings**: Abre as **configurações do SNGREP**, incluindo **interface, opções de captura, opções de fluxo de chamada e configurações EEP/HEP Homer**.
- **F10**: Permite **escolher quais colunas serão exibidas** na janela do **sngrep**.

SPAM?

image

- **User-Agent**: A maioria das tentativas de **spam** mostra um **User-Agent indesejado**, como o exibido neste exemplo.

Registration

image

image

Registration Expanded

image

image

Call Setup

image

image

Invite

image

200 OK

image

Call completou

image

image

F3 Search

image

F7 Filtro

image

F8 Configurações

Interface

image

EEP/HEP HOMER

image

Call Flow

image

Capture

image

Revision #3
Created 23 February 2026 20:38:19 by Matheus Lima
Updated 13 April 2026 18:59:43 by Matheus Lima