



 Manual do Usuário SharpShark

Sistema de Análise de Tráfego e Segurança de Rede

## **Seção 1: Instalação e Primeira Execução**

Bem-vindo ao SharpShark. Este guia pressupõe que você já tenha o **Docker Desktop** (ou Docker + Docker Compose) instalado e funcionando em sua máquina.

A instalação é feita em três comandos simples.

## 1.1. Baixar e Subir os Containers

Primeiro, clone o repositório principal e inicie os serviços com docker-compose. Este comando irá construir o backend (Python/TShark), o frontend (React/Nginx), criar os volumes de dados e iniciar tudo.

### a) Clone o repositório

```
git clone https://github.com/MateuzCabral/SharpShark-Monorepo.git  
cd SharpShark-Monorepo
```

**b) Construa e inicie os containers**

```
docker-compose up -d --build
```

Após o build, o terminal deve mostrar que os containers `sharpshark_backend` e `sharpshark_frontend` foram iniciados ("Started") e os volumes (`_db`, `_uploads`, `_pcaps`) foram criados.

```
>>> CACHED [frontend] builder 4/6 RUN npm install
>>> CACHED [frontend] builder 5/6 COPY .
>>> CACHED [frontend] builder 6/6 RUN npm run build
>>> CACHED [frontend] stage-1 2/31 COPY --from=builder /app/dist /usr/share/nginx/html
>>> CACHED [frontend] stage-1 3/31 COPY nginx.conf /etc/nginx/conf.d/default.conf
>>> CACHED [backend] 2/10 RUN apt-get update && apt-get -y upgrade && rm -rf /var/lib/apt/lists/*
>>> CACHED [backend] 3/10 WORKDIR /app
>>> CACHED [backend] 4/10 COPY app/requirements.txt
>>> CACHED [backend] 5/10 RUN pip install --no-cache-dir -r requirements.txt
>>> CACHED [backend] 6/10 COPY app/
>>> CACHED [backend] 7/10 COPY entrypoint.sh .
>>> CACHED [backend] 8/10 COPY .env-example .
>>> CACHED [backend] 9/10 RUN chmod +x entrypoint.sh
>>> CACHED [backend] 10/10 RUN chmod +r app/uploads
[frontend] exporting to image
>>> CACHED [frontend] 1/1 FROM alpine:3.11
>>> CACHED [frontend] 2/1 EXPORT manifest sha256:058542e1d63ab315a1c2a0f13595dc1b9a7fa640221f191d0e8588204ddcdcc6603
>>> CACHED [frontend] 3/1 EXPORT config sha256:18293f71e6f5699de961975b3e3la1bc866523c3826e5be2ec3d259fc7b63
>>> CACHED [frontend] 4/1 EXPORT attestation manifest sha256:f0893a31e6d25e3b16e99d329ff2fb15e89421d7a8c4933550069c88923e
>>> CACHED [frontend] 5/1 EXPORT manifest list sha256:a9103940c5c24ef0d66e940486652294ed868aa0fce26f289c888a98872dad8
>>> CACHED [frontend] 6/1 EXPORT image sha256:18293f71e6f5699de961975b3e3la1bc866523c3826e5be2ec3d259fc7b63
>>> CACHED [backend] 1/1 FROM docker.io/library/sharpshark:Frontend:latest
[backend] exporting to image
>>> CACHED [backend] 1/1 FROM alpine:3.11
>>> CACHED [backend] 2/1 EXPORT layers sha256:b13efbd7f01b1836390a2c0268aa811a664765bf5063cf6c9fc4ff294ff7f688
>>> CACHED [backend] 3/1 EXPORT config sha256:17206927232c353d779eb7a2dd94bf1fe6669542477ccb5a1eac8a777
>>> CACHED [backend] 4/1 EXPORT attestation manifest sha256:0772a7c92a72b30596d0838623bfdbf8eac2239324f601d1dafa7u076fd5
>>> CACHED [backend] 5/1 EXPORT image sha256:17206927232c353d779eb7a2dd94bf1fe6669542477ccb5a1eac8a777
>>> CACHED [backend] 6/1 UNPACKAGING to docker.io/library/sharpshark:Backend:latest
[backend] resolving provenance for metadata file
>>> CACHED [backend] 1/1 FROM alpine:3.11
[backend] resolving provenance for metadata file
[backend] 1/1 RUN g/6
sharpshark-backend          Built
sharpshark-frontend         Built
sharpshark-monorepo_sharpshark_db Created
sharpshark-monorepo_sharpshark_uploads Created
Containsharpshark_backend   Started
Containsharpshark_frontend  Started
```

## 1.2. Criar seu Usuário Administrador

Com os containers em execução, o servidor está no ar, mas o banco de dados está vazio. Você precisa criar seu primeiro usuário administrador.

Abra o terminal na mesma pasta e execute:

```
docker-compose exec backend python3 -m cli create-admin
```

O terminal ficará interativo. Siga as instruções para criar seu usuário:

1. **Nome do usuário:** Digite o nome do seu admin (ex: admin).
2. **Senha (mínimo 8 caracteres):** Digite sua senha (ela ficará oculta).
3. **Repeat for confirmation:** Digite a senha novamente.

O sistema confirmará a criação com a mensagem: Sucesso! Administrador 'admin' criado.

```
--- Criando Novo Administrador SharpShark ---
Nome do usuário: admin
Senha (mínimo 8 caracteres):
Repeat for confirmation:
Sucesso! Administrador 'admin' criado.
```

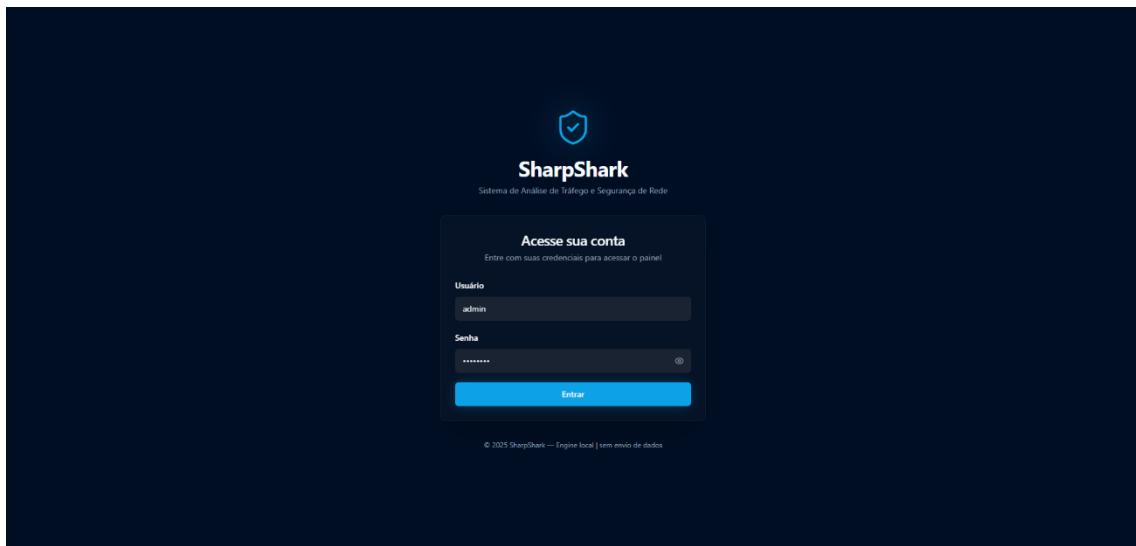
---

## Seção 2: Acesso ao Sistema e Visão Geral

### 2.1. Acessando o Painel (Login)

Sua instalação está completa.

1. Abra seu navegador (Chrome, Firefox, Edge, etc.).
2. Na barra de endereços, digite: http://localhost e pressione Enter.
3. Você verá a tela de login do SharpShark. Use as credenciais de administrador que você criou no passo anterior para entrar.



### 2.2. O Dashboard (Visão Geral)

Ao fazer login, você é recebido pelo Dashboard, que fornece uma visão geral de alto nível do seu ambiente de rede.

O dashboard é composto por:

- **Cards de Estatísticas:** Um resumo rápido do número total de pacotes analisados, alertas de segurança encontrados, IPs únicos registrados e análises concluídas.
  - **Gráfico de Tráfego:** Mostra a atividade da rede (pacotes por hora) nas últimas 24 horas, permitindo identificar picos de atividade.
  - **Gráfico de Protocolos:** Um gráfico de pizza que mostra a distribuição dos protocolos mais comuns (ex: TCP, FTP, HTTP) em todo o tráfego analisado.
  - **Alertas Recentes:** Uma tabela com os últimos alertas detectados pelo sistema.
- 

### Seção 3: Gerenciamento (Painel de Admin)

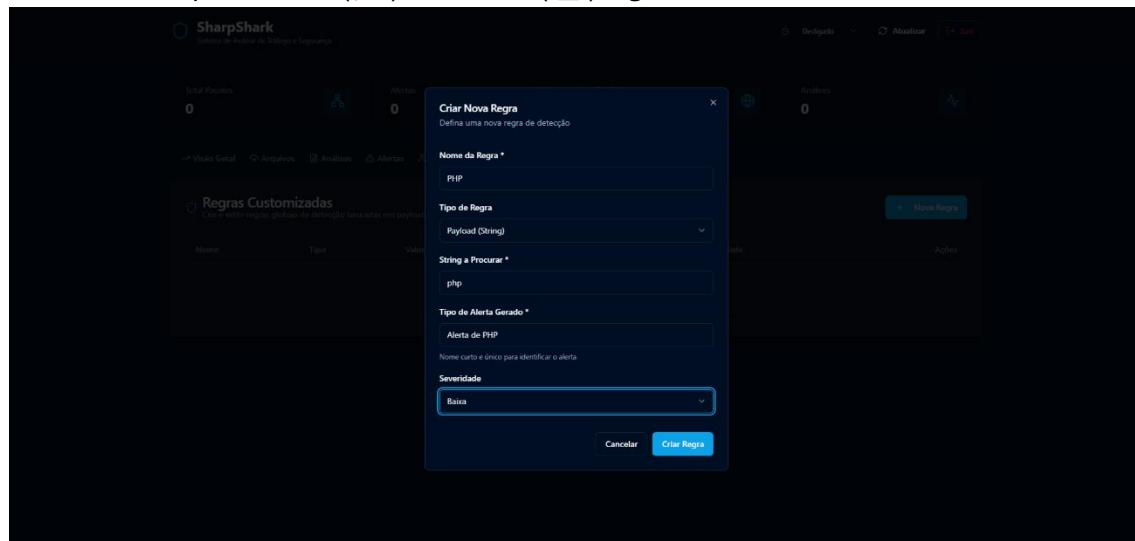
Como administrador, você tem acesso a abas adicionais para configurar o sistema.

#### 3.1. Gerenciamento de Regras (Aba "Regras")

Aqui você pode criar suas próprias regras de detecção.

1. Vá para a aba "**Regras**" e clique em "Nova Regra".
2. Um modal (como o da imagem) aparecerá.
3. **Nome da Regra:** Um nome amigável (ex: PHP).
4. **Tipo de Regra:**
  - Payload (String): O sistema procurará por essa string exata (ex: php) no conteúdo dos pacotes e streams.
  - Porta: O sistema alertará sobre qualquer tráfego para uma porta específica (ex: 4444).
5. **Tipo de Alerta Gerado:** Um nome técnico para o alerta (ex: Alerta de PHP).
6. **Severidade:** Defina o nível de risco (ex: Baixa).
7. Clique em "Criar Regra".

Você também pode editar (✎) ou deletar (🗑) regras existentes nesta aba.

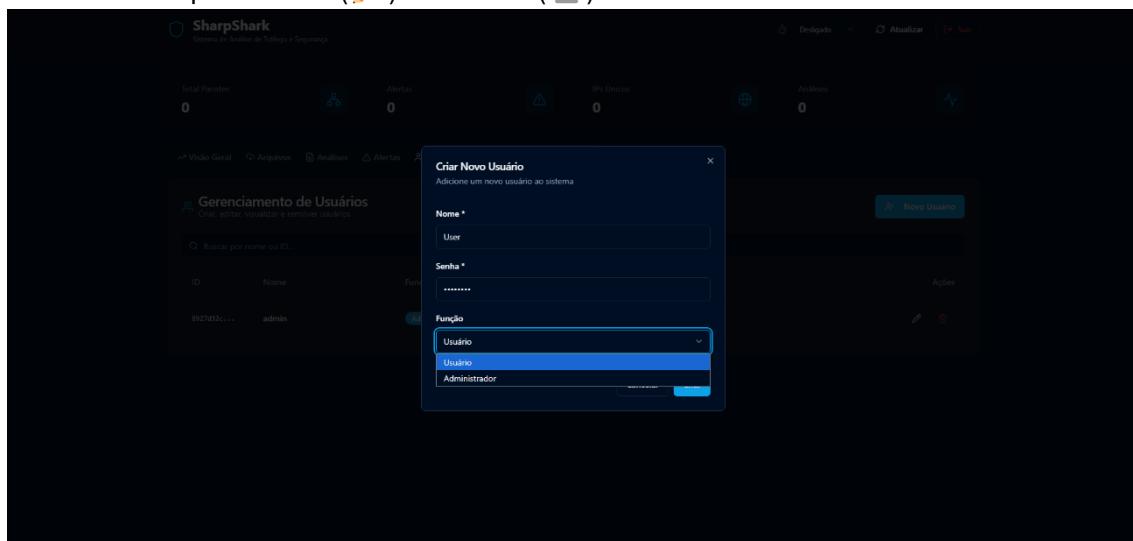


### 3.2. Gerenciamento de Usuários (Aba "Usuários")

Aqui você pode gerenciar quem acessa o sistema.

1. Vá para a aba "**Usuários**" e clique em "Novo Usuário".
2. Preencha o **Nome** e a **Senha** (mínimo 8 caracteres).
3. **Função:** Esta é a permissão mais importante:
  - Usuário: Pode ver análises e dashboards, mas não pode gerenciar usuários, regras ou configurações.
  - Administrador: Tem acesso total ao sistema.
4. Clique em "Criar".

Você também pode editar (📝) ou deletar (🗑) usuários existentes nesta aba.



---

## Seção 4: Fluxo de Análise (Manual)

Esta seção cobre o fluxo de uso mais comum: fazer o upload de um arquivo .pcap/.pcapng e analisar seus resultados.

### 4.1. Passo 1: Fazer o Upload do Arquivo

1. No menu de navegação, clique na aba "**Arquivos**".
2. No card "**Upload Manual**", clique em "Escolher arquivo" e selecione um arquivo .pcap ou .pcapng do seu computador.
3. Clique em "Enviar Arquivo".
4. O sistema mostrará uma notificação de "Upload concluído".
5. O arquivo aparecerá no "**Histórico Recente de Uploads**" com status "Sucesso" e também será adicionado à tabela principal de "**Arquivos Enviados**".

#### 4.2. Passo 2: Acompanhar a Análise

1. Clique na aba "Análises".
2. Você verá que o arquivo enviado (ex: Capture\_...pcapng) aparece na lista. O status pode estar como "Pendente" ou "Processando".
3. Após a conclusão, o status mudará para "Concluída".
4. Note que os **Cards de Estatísticas** no topo da página serão atualizados com os dados desta nova análise (ex: 907 Pacotes, 4 Alertas).

#### 4.3. Passo 3: Ver Detalhes da Análise

Na aba "Analises", clique no ícone de olho (👁️) na linha da análise concluída. Você será levado à página de "Detalhes da Análise".

Esta página é dividida em quatro seções:

**1. Sumário da Análise:** Mostra os metadados principais do arquivo: Status, Duração da análise, Total de Pacotes, Streams Salvos e o Hash SHA256 completo do arquivo.

Capture\_1612220005488\_20251105T174447932.pcapng  
18625763-9fec-4193-9111-1ef8436decc655

**Sumário da Análise**

STATUS	DURAÇÃO	PACOTES	STREAMS SALVOS
Concluída	0.83 seg	907	21
TAMANHO	ANALISADO EM	HASH (SHA256)	
0.1 MB	05/11/2025, 14:44:48	96fa774b82ea249fe1c84c84e25c180331b2f130fffb3f99a29c1255acdf78683	

**Estatísticas da Análise**  
Protocolos, Portas e outros dados agregados desta análise.

Protocolos	Portas																
<table border="1"><thead><tr><th>Item</th><th>Contagem</th></tr></thead><tbody><tr><td>TCP</td><td>635</td></tr><tr><td>FTP.CURRENT-WORKING-DIRECTORY</td><td>109</td></tr><tr><td>TCP.SEGMENTS</td><td>90</td></tr></tbody></table>	Item	Contagem	TCP	635	FTP.CURRENT-WORKING-DIRECTORY	109	TCP.SEGMENTS	90	<table border="1"><thead><tr><th>Item</th><th>Contagem</th></tr></thead><tbody><tr><td>80</td><td>461</td></tr><tr><td>53734</td><td>444</td></tr><tr><td>21</td><td>430</td></tr></tbody></table>	Item	Contagem	80	461	53734	444	21	430
Item	Contagem																
TCP	635																
FTP.CURRENT-WORKING-DIRECTORY	109																
TCP.SEGMENTS	90																
Item	Contagem																
80	461																
53734	444																
21	430																

**Endereços IP**  
Top 10 IPs de origem e destino encontrados nesta análise.

Top 10 IPs de Origem (Top 2)	Top 10 IPs de Destino (Top 2)
192.168.0.147	192.168.0.115
192.168.0.115	192.168.0.147

**2. Estatísticas da Análise:** Tabelas que detalham os principais **Protocolos** e **Portas** encontrados na captura, ordenados por contagem.

**3. Endereços IP:** Tabelas com o Top 10 de IPs de Origem (quem envia) e IPs de Destino (quem recebe) mais ativos na captura.

**4. Alertas da Análise:** A seção mais importante. É uma tabela com todos os alertas de segurança e anomalias que o SharpShark encontrou *especificamente* neste arquivo. Os alertas são classificados por severidade (Low, Medium, High, Critical).

**Endereços IP**  
Top 10 IPs de origem e destino encontrados nesta análise.

Top 10 IPs de Origem (Top 2)	Top 10 IPs de Destino (Top 2)
192.168.0.147	192.168.0.115
192.168.0.115	192.168.0.147

**Alertas da Análise**  
Todos os alertas gerados especificamente para esta análise.

Tipo	Severidade	IP Origem	IP Destino	Porta	Protocolo	Ações
Alerta de PHP	Low	192.168.0.115	192.168.0.147	50339	Stream (TCP)	🔗
Alerta de PHP	Low	192.168.0.147	192.168.0.115	21	FTP.CURRENT-WORKING-DIRECTORY	🔗
Comunicação FTP	Medium	192.168.0.147	192.168.0.115	21	TCP	🔗
brute.force.detected	Critical	192.168.0.147	192.168.0.115	21	FTP.CURRENT-WORKING-DIRECTORY	🔗

#### 4.4. Passo 4: Investigar um Alerta Específico

Na tabela "Alertas da Análise", clique no ícone de olho (👁️) de um alerta para investigá-lo.

Um modal de "Detalhes do Alerta" aparecerá, mostrando:

- Metadados:** IPs, Portas, Protocolo e Severidade do alerta.
- Evidência:** A razão pela qual o alerta foi gerado.

- **Conteúdo do Stream:** A "prova" do alerta. O SharpShark reconstrói o fluxo de comunicação e exibe o payload de texto plano que causou a detecção.

**Exemplo 1: Regra Customizada (Baixa Severidade)** Neste exemplo, o sistema detectou a string "php", que correspondia a uma regra customizada. O conteúdo do stream mostra o código-fonte de um *reverse shell* em PHP.

The screenshot shows the SharpShark interface with several panels. On the left, there's a sidebar titled 'Alertas da Análise' listing alerts such as 'Alerta de PHP' (Severity: Low), 'Alerta de PHP' (Severity: Low), 'Comunicação FTP' (Severity: Medium), and 'brute\_force\_detected' (Severity: Critical). The main area has two tabs: 'Top 10 IPs de Origem (Top 2)' and 'Top 10 IPs de Destino (Top 2)'. In the center, a modal window titled 'Detalhes do Alerta' displays information about the 'Alerta de PHP' alert. It shows the type as 'Alerta de PHP', severity as 'Low', IP Origem as '192.168.0.147', IP Destino as '192.168.0.115', Porta as '50339', and Protocolo as 'Stream (TCP)'. The analysis ID is '18025783-9fec-4193-9211-2f9436dec658'. The evidence section contains the text: 'Assinatura de stream (Regras: PHP) encontrado: "php"' followed by the PHP reverse shell code. The content of the stream (Texto Plano) shows the same code. To the right, there's a 'Contagem (Pacotes)' panel showing 479 packages for the source and 428 for the destination, with a list of files like 'p DIRECTORY' and 'q DIRECTORY'.

**Exemplo 2: Detecção do Sistema (Crítica Severidade)** Neste exemplo, o sistema detectou um ataque de *brute\_force\_detected* (força bruta). A evidência mostra o número de tentativas de login falhas, e o conteúdo do stream exibe a conversa FTP completa, incluindo as múltiplas falhas (Login incorrect.) seguidas de um Login successful.

This screenshot shows the same SharpShark interface as the previous one. The 'Alertas da Análise' sidebar now lists 'brute\_force\_detected' (Severity: Critical) as the most recent alert. The central 'Detalhes do Alerta' modal for this alert shows the type as 'brute\_force\_detected', severity as 'Critical', IP Origem as '192.168.0.147', IP Destino as '192.168.0.115', Porta as '21', and Protocolo as 'FTP,CURRENT-WORKING-DIRECTORY'. The analysis ID is '18025783-9fec-4193-9211-2f9436dec658'. The evidence section shows 'Detetadas 11 tentativas de login falhados de 192.168.0.147 para 192.168.0.115/21'. The content of the stream (Texto Plano) shows the FTP session logs, including multiple failed login attempts ('331 Please specify the password.', 'PASS password123') and one successful login ('230 Login successful.').

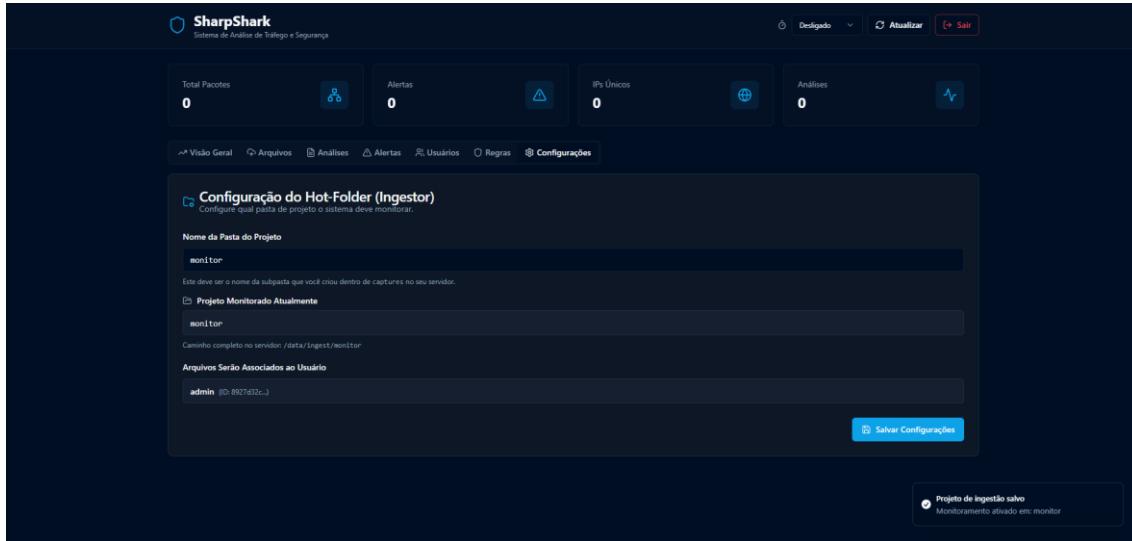
## Seção 5: Guia Avançado - Configurando o "Hot-Folder" (Ingestão Automática)

Esta é a funcionalidade mais poderosa do SharpShark. Ela permite que o sistema monitore uma pasta e analise arquivos .pcapng automaticamente.

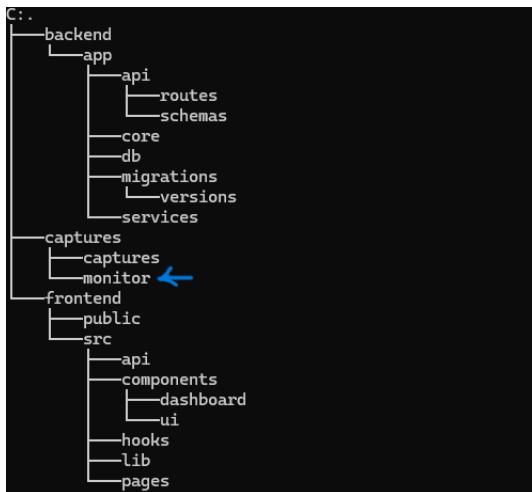
A configuração é feita em duas partes: **no SharpShark** e no **Wireshark**.

### 5.1. Parte 1: Configurar o SharpShark (UI)

1. Acesse a aba "**Configurações**".
2. No campo "**Nome da Pasta do Projeto**", digite um nome simples para sua pasta de monitoramento. Exemplo: monitor.
3. Clique em "**Salvar Configurações**".



O sistema irá automaticamente criar esta pasta para você. No *host* do Docker (seu computador), dentro da pasta do projeto (SharpShark-Monorepo/), você verá que a pasta captures/monitor/ foi criada. O SharpShark agora está monitorando este local.



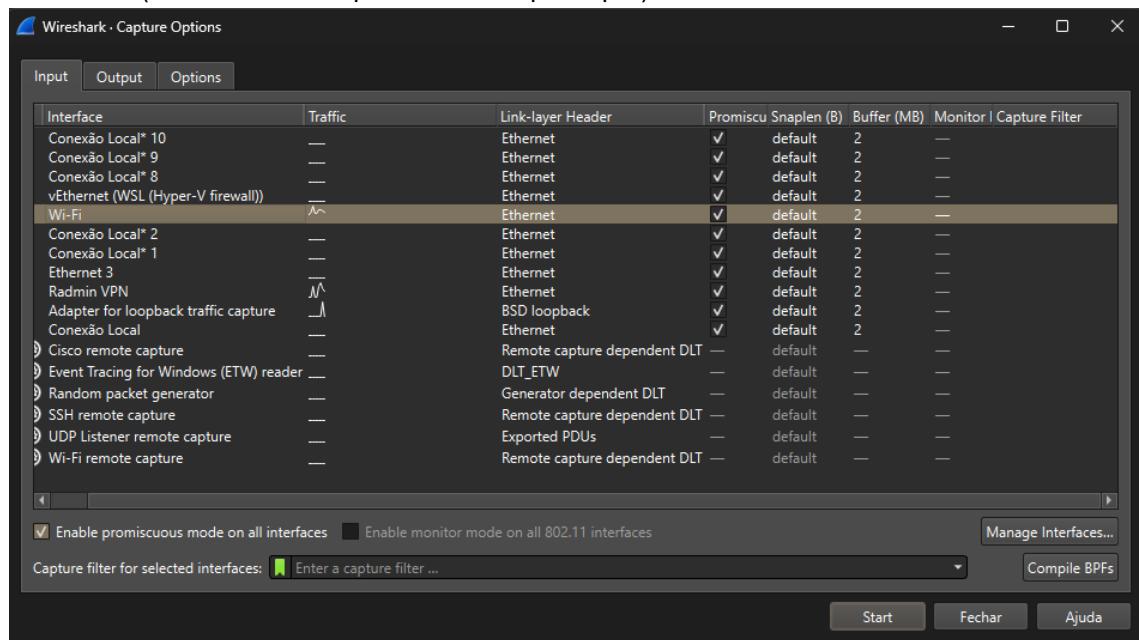
## 5.2. Parte 2: Configurar o Wireshark (para salvar os arquivos)

Agora, precisamos dizer ao Wireshark (ou tcpdump) para salvar os arquivos de captura automaticamente *dentro* dessa pasta que acabamos de criar.

**Passo 1:** No Wireshark, vá ao menu Capture (Captura) e selecione Options... (Opções...).

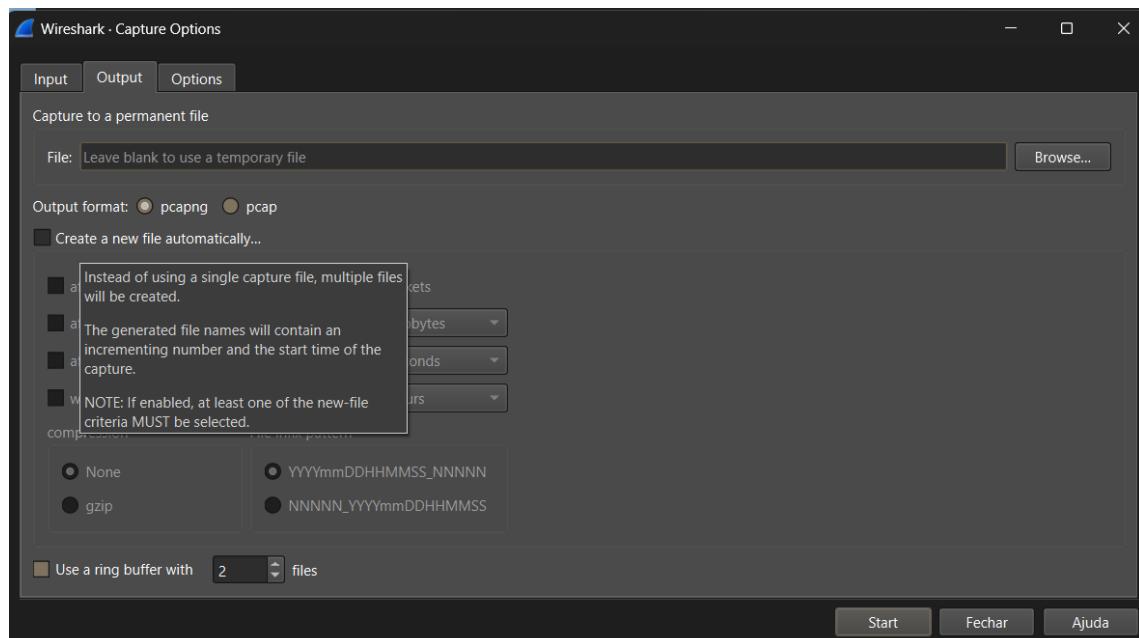


**Passo 2:** Na aba "Input" (Entrada), selecione a interface de rede que você deseja monitorar (ex: Wi-Fi ou sua placa de rede principal).

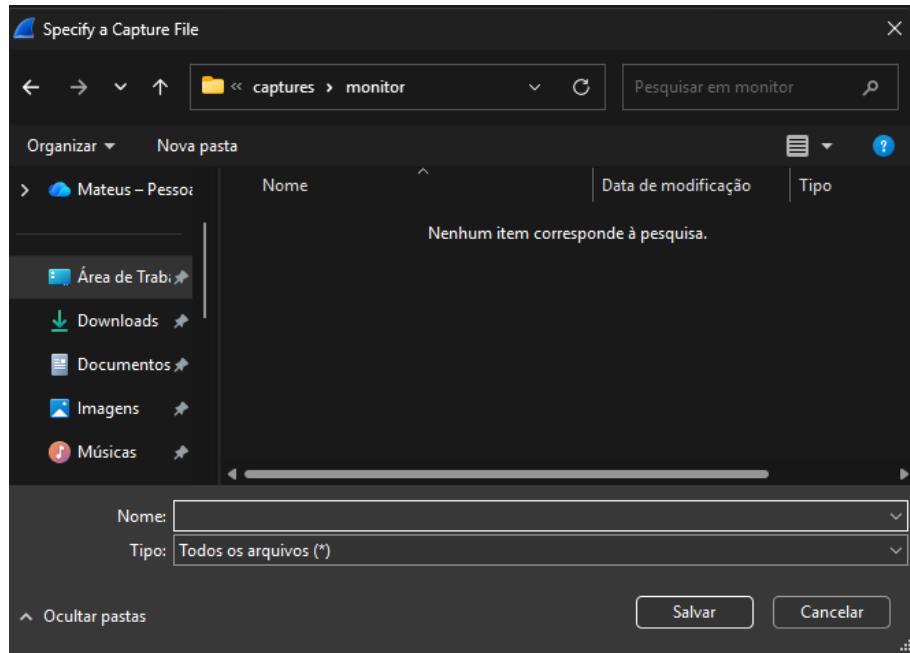


**Passo 3:** Clique na aba "Output" (Saída).

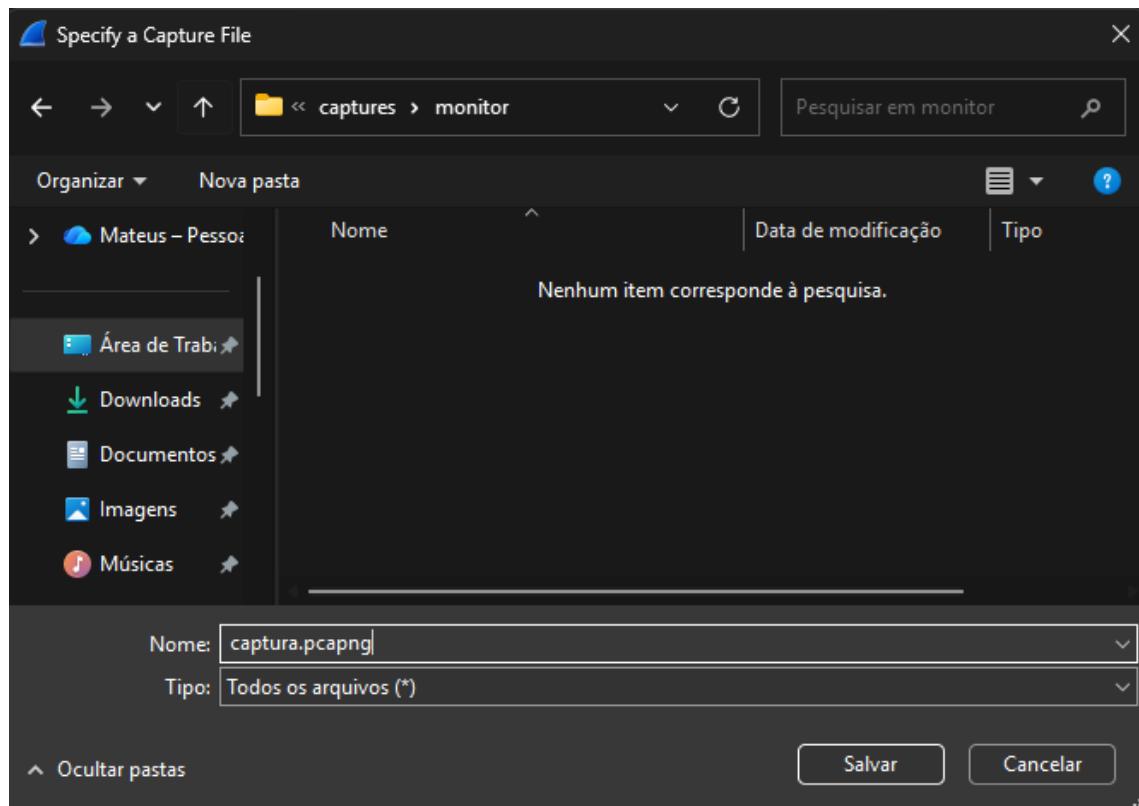
- Clique em "Browse..." (Procurar...).



- Navegue até a pasta do seu projeto e entre na pasta captures/ e, em seguida, na subpasta que você criou (ex: captures/monitor).



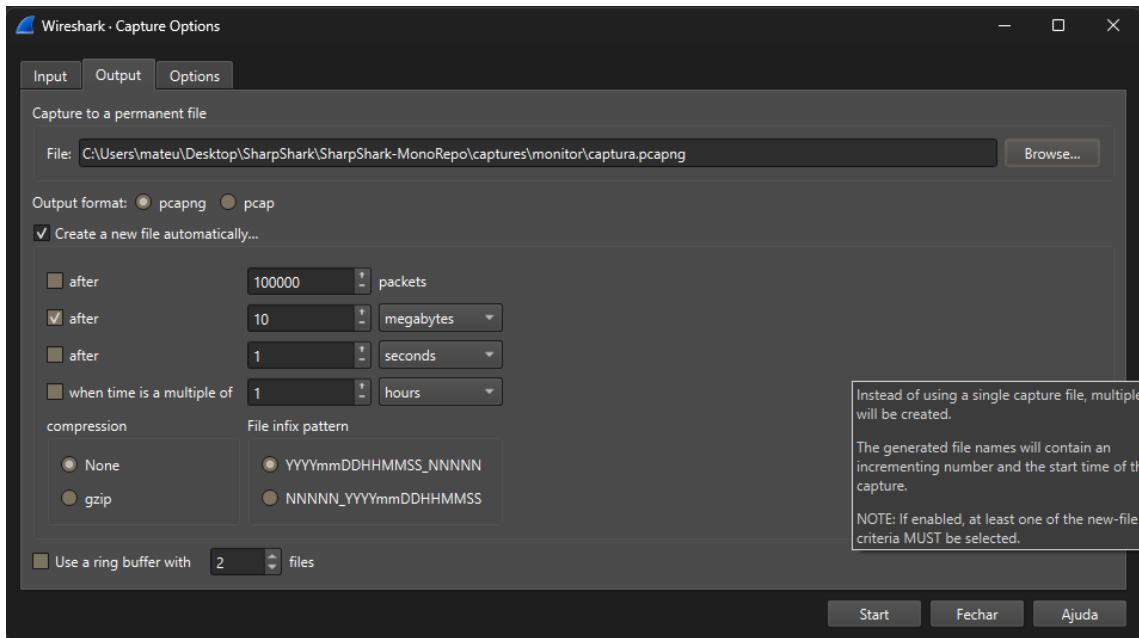
- No campo "**Nome**", dê um nome base para seus arquivos, como `captura.pcapng`.
- Clique em "**Salvar**".



**Passo 4:** De volta à tela "Output", configure a rotação de arquivos.

- Marque a caixa "**Create a new file automatically...**" (Criar um novo arquivo automaticamente...).

- Selecione um critério para "fechar" um arquivo e criar o próximo. Recomendamos usar after 10~50 megabytes (a cada 10 ou 50 MB), mas o sistema suporta até 100 MB.
- Verifique se o **"Output format"** está correto (ex: pcapng).
- Clique em **"Start"**.



## 6. Conclusão

Pronto! O Wireshark agora está capturando o tráfego da sua rede, salvando um novo arquivo de acordo com as opções escolhidas na pasta captures/monitor. O ingestor do SharpShark irá detectar cada novo arquivo, processá-lo e adicionar os resultados ao seu dashboard automaticamente.