Apresentação
WIRESHARK

CARLA BEATRIZ
KLAYRTON VASCONCELOS
JHONATAN SILVA

O que é o Wireshark?

Wireshark é um analisador de protocolo de rede criado por Gerald Combs em 1998 que permite capturar e navegar interativamente no tráfego em execução em uma rede de computadores. Possui um conjunto de recursos rico e poderoso e é a ferramenta desse tipo mais popular do mundo, por possuir um código aberto e gratuito que consegue atuar em diversos tipos de Sistemas Operacionais (Windows, Linux, MacOS)

Características Principais

- Inspeção profunda de centenas de protocolos
- Captura ao vivo e análise offline.
- Suporte de descriptografia para muitos protocolos, incluindo IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP e WPA/WPA2.
- Os arquivos de captura compactados com gzip podem ser descompactados instantaneamente.
- A saída pode ser exportada para XML, PostScript®, CSV ou texto simples.

Propósito

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam eget quam lacus. Vivamus laoreet tempus lacus, in ultricies dui vehicula in. Donec auctor blandit leo. convallis mollis mi condimentum in.

Como funciona?

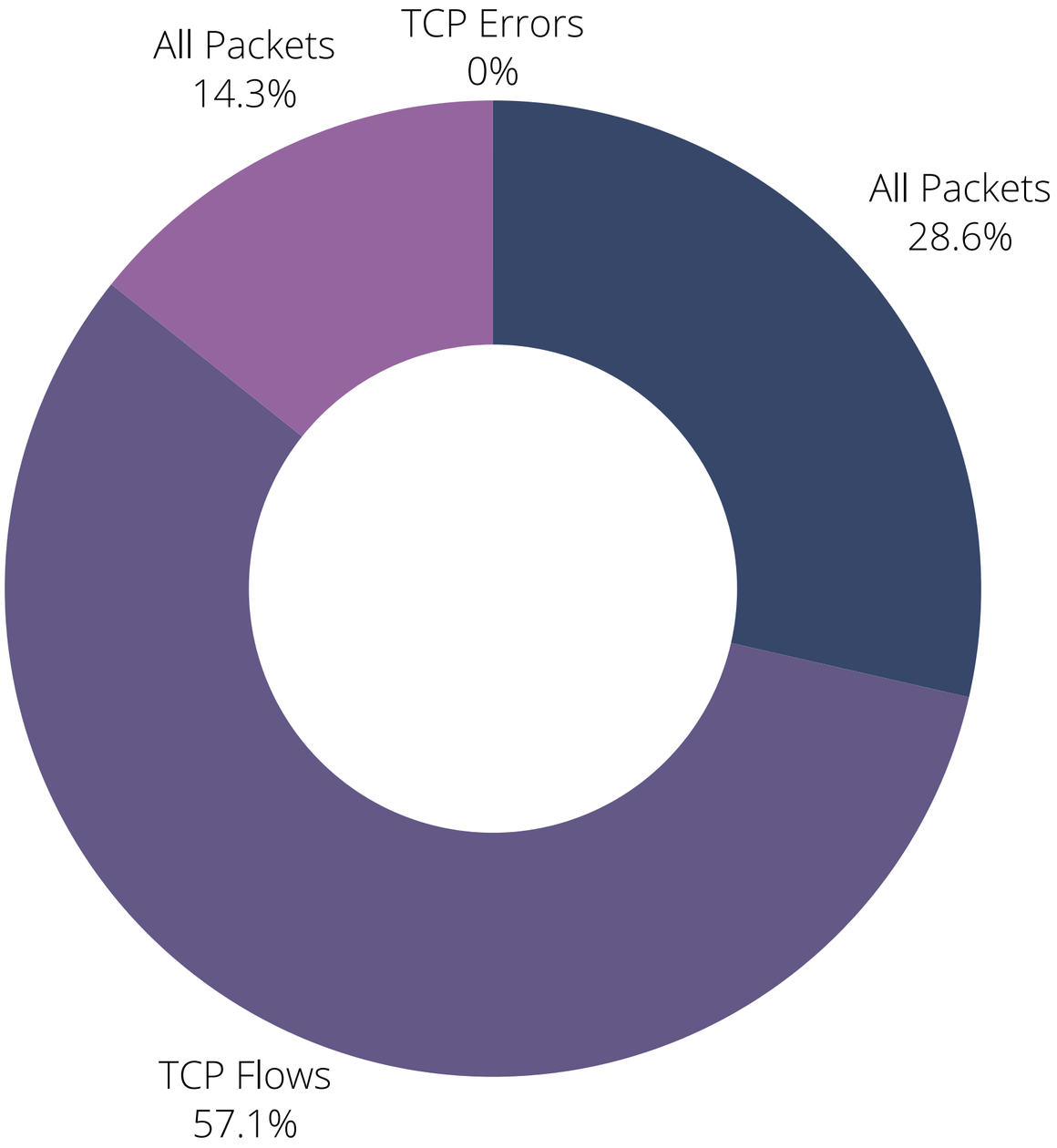
Atua fazendo captura o tráfego de rede e armazenar esses dados para análise offline. O Wireshark captura o tráfego de rede Ethernet, Bluetooth, sem fio (IEEE.802.11), token ring, conexões frame relay, entre outros.

A ferramenta realiza filtragem do log antes do início da captura ou durante a análise. Possibilitando a configurarção do filtro para análise de pacotes enviados e recebidos Os filtros no Wireshark são um dos principais motivos que fizeram dele a ferramenta padrão para análise de pacotes.

O Wireshark disponibiliza uma interface de linha de comando (ILC), caso o seu um sistema operacional não tenha uma GUI. O recomendado seria usar a ILC para capturar e salvar um log e, assim, revisar esse log com a GUI.

Tipos de Dados Capturados

DADOS DE PROTOCOLO	O Wireshark captura os dados brutos de protocolos, incluindo o cabeçalho do pacote e a carga útil. Tais dados são usados para compreender a mecânica dos protocolos de rede, bem como para compreender os dados que são transferidos pela rede.
DADOS DE APLICAÇÃO	O Wireshark é capaz de capturar vários tipos de dados de aplicativos, incluindo conteúdo de e-mail, páginas da web e arquivos transferidos. Esses dados são altamente benéficos para solucionar quaisquer problemas que possam surgir com os aplicativos e monitorar rede.
DADOS DE DIAGNÓSTICO	O Wireshark também pode capturar dados de diagnósticos, como informações de desempenho, erros de rede e alertas de segurança. Esses dados são úteis para identificar problemas de rede e garantir a segurança e confiabilidade.



Ferramentas de Análise

CAPTURA DOS PACOTES:

Permite que o usuário consiga visualizar todo o tráfego de determinada rede em tempo real e captar os picos de consumo;

GRÁFICOS E ESTATÍSTICAS:

Fornece informações em imagem e dados que permitem uma análise mais criteriosa e fácil do fluxo de rede e seus pacotes capturados;

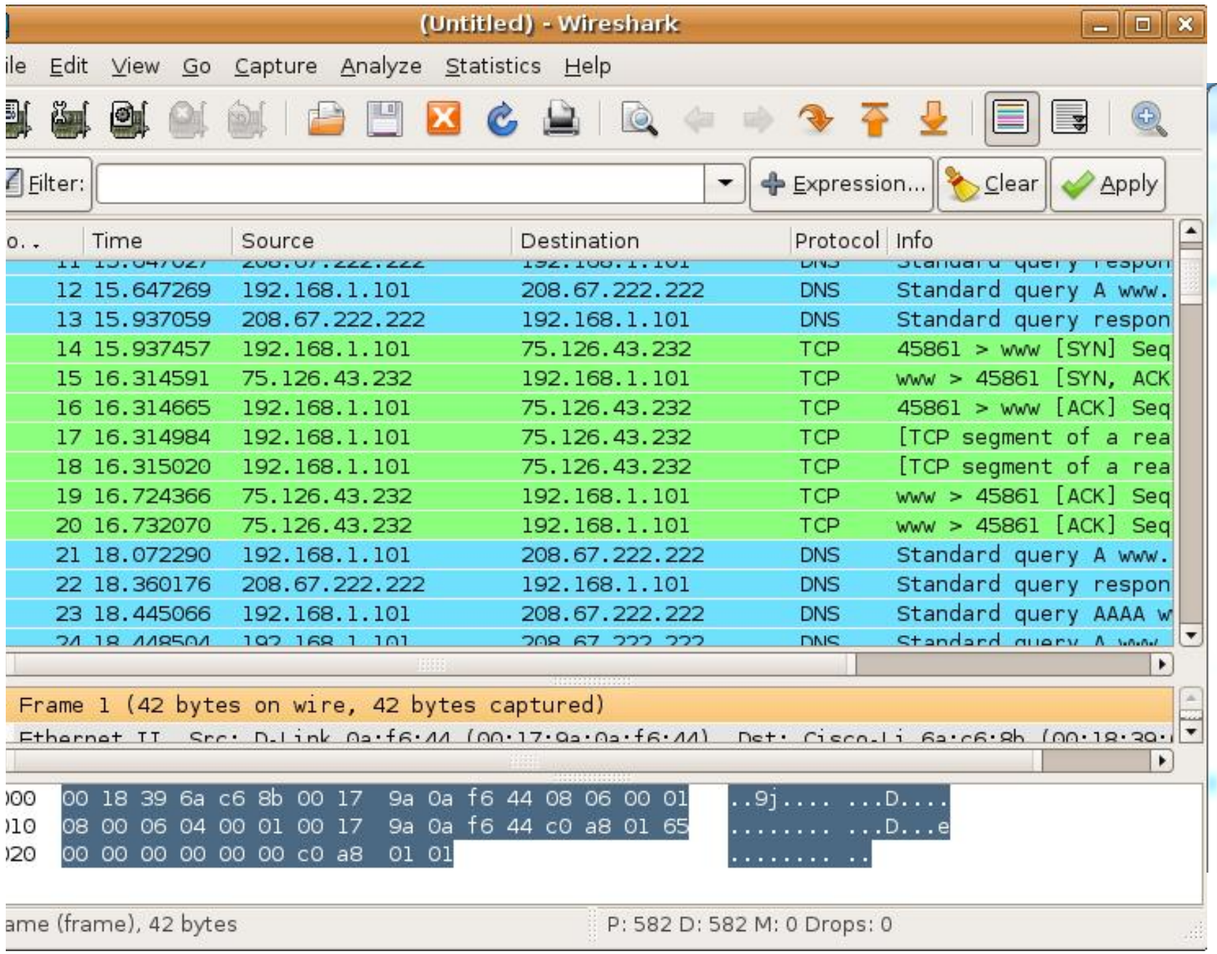
AGRUPAMENTOS

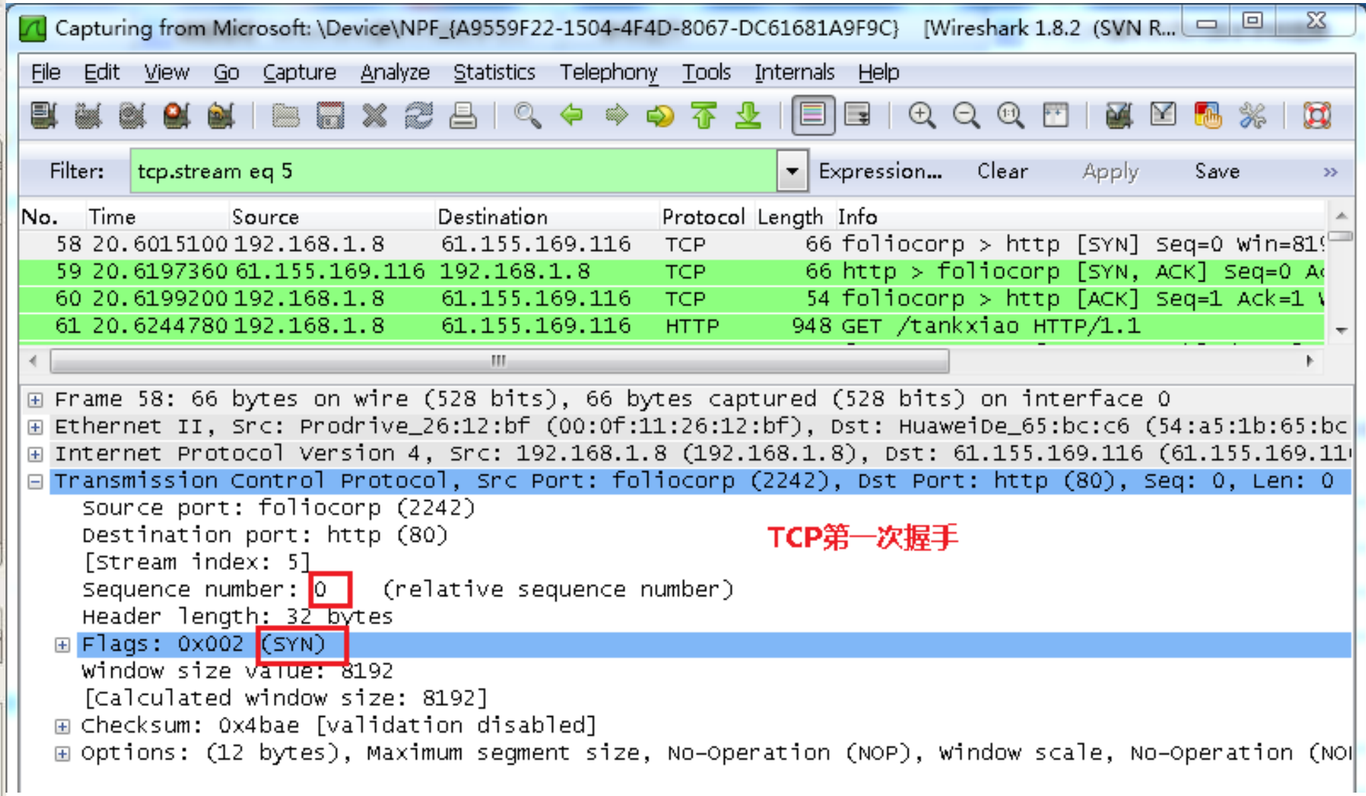
Permite que sejam agrupados pacotes que possuem um fluxo específico;

DECODIFICAÇÃO DOS PACOTES

Os pacotes capturados são decodificados permitindo que se obtenha informações detalhadas de cada pacote e seus protocolos.

Amostras de Capturas

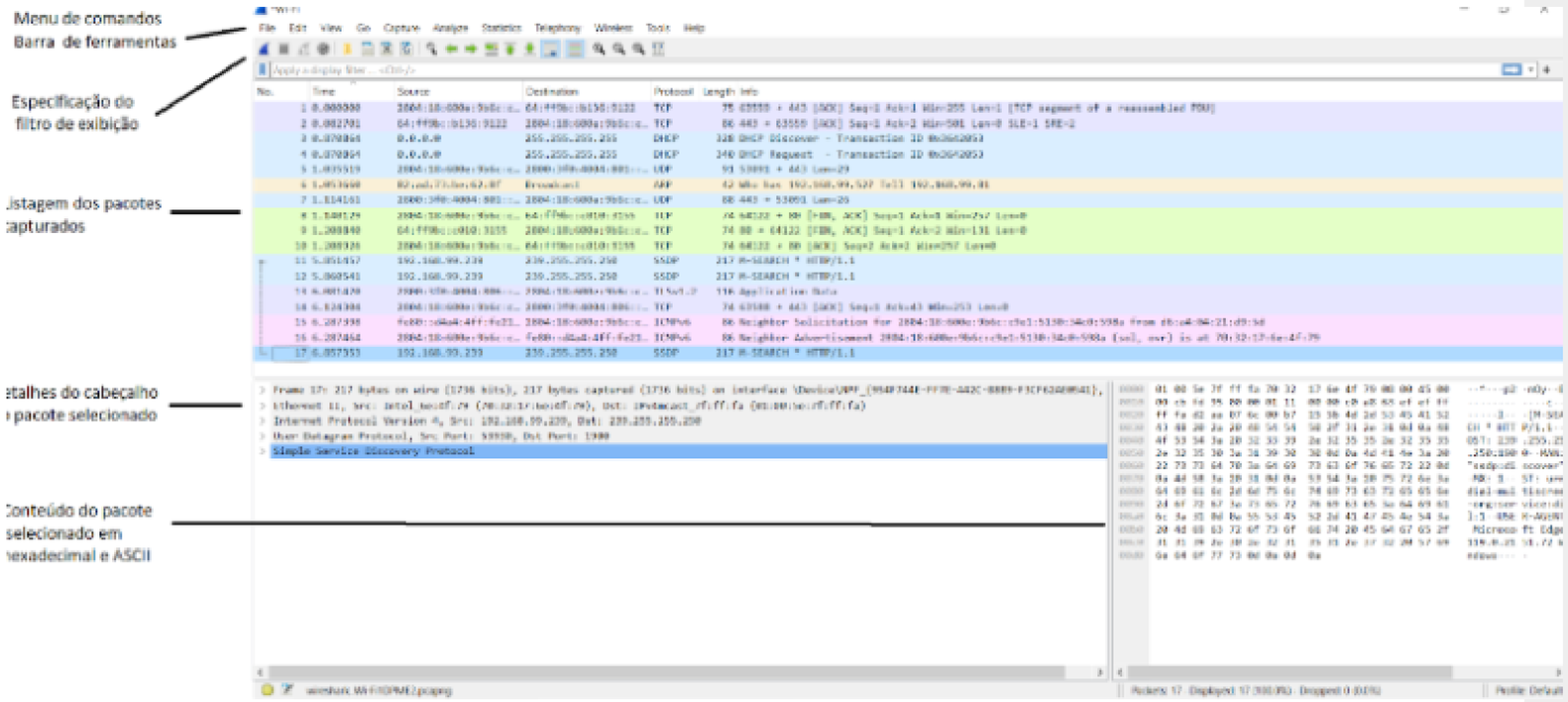




Tipos de Buscas e Filtragens

REDE LOCAL	É possível fazer a restrição no programa para que se trabalhe apenas dentro do tráfego da rede local, reduzindo assim a quantidade de informações a serem analisadas pelo usuário.
PORTAS TCP/UDP	É possível fazer essa filtragem de pacotes usando como referência a porta que está sendo utilizada na transação dos pacotes enviados.
IP ORIGEM DESTINO	É possível fazer a filtragem dos pacotes através do IP de origem e destino da rota do pacote

Capturas



ITEM 1

O Wireshark captura apenas pacotes destinados ao computador no qual está instalado. Para capturar pacotes que passam por um switch ou servidor, é necessário configurar o switch/servidor para enviar uma cópia de todos os quadros para uma porta específica.

Ao iniciar a captura, podemos ver que a máquina realizou várias requisições, como buscas de endereços utilizando o protocolo ARP, pedido de um endereço IP utilizando protocolo DHCP, transferência de arquivos com o protocolo UDP e ICMP para informar erros de transmissão de dados.

Observando o campo “listagem de pacotes”, temos um cabeçalho do programa onde podemos organizar os pacotes por time(tempo), origem(source), destination(destinatário), protocol(protocolo) , length(comprimento do pacote) e info(descrição). Além de organizar pelo cabeçalho do programa podemos ter uma visualização utilizando as cores por tipo de pacote.

Usabilidade da ferramenta no Mercado

Administração de Sistemas
Utilizado para analisar, diagnosticar problemas e permitir que o time de sistemas atue em melhorias e otimizações dentro das corporações com intuito de melhorar o desempenho e qualidade do serviço

Redes e Segurança
Utilizado por equipes de TI voltadas para área de rede e segurança, com foco de analisar o tráfego de dados, detectção de ameaças e riscos naquele ambiente, assim como incrementação de novas políticas de segurança para melhoria do fluxo

Desenvolvimento de software
A área de desenvolvimento utiliza a ferramenta com objetivo de melhorar aplicativos de monitoramento de utilizam ou dependem do programa para obtenção das informações de rede

OBRIGADO!

Carla Beatriz da Silva Teixeira

Francisco Klayrton Vasconcelos

Jhonatan Silva de Sousa