

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 descryptografia 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 configuração 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

CAPURA 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:

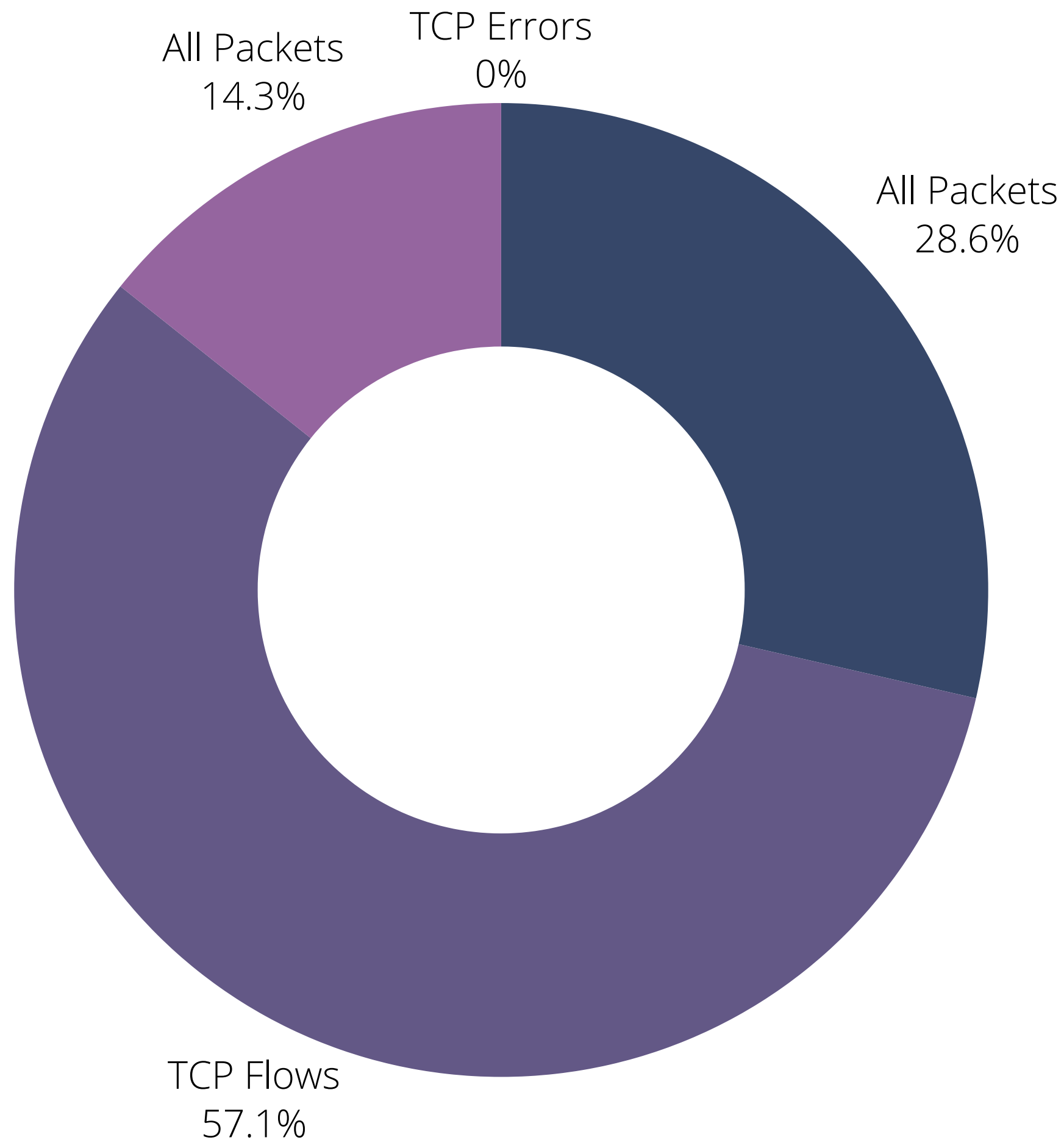
Fornecer informações em imagem e dados que permitem uma análise mais criteriosa e fácil do fluxo de rede e seus pacotes capturados;

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

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
11	15.047027	208.67.222.222	192.168.1.101	DNS	Standard query response
12	15.647269	192.168.1.101	208.67.222.222	DNS	Standard query A www.
13	15.937059	208.67.222.222	192.168.1.101	DNS	Standard query response
14	15.937457	192.168.1.101	75.126.43.232	TCP	45861 > www [SYN] Seq
15	16.314591	75.126.43.232	192.168.1.101	TCP	www > 45861 [SYN, ACK
16	16.314665	192.168.1.101	75.126.43.232	TCP	45861 > www [ACK] Seq
17	16.314984	192.168.1.101	75.126.43.232	TCP	[TCP segment of a rea
18	16.315020	192.168.1.101	75.126.43.232	TCP	[TCP segment of a rea
19	16.724366	75.126.43.232	192.168.1.101	TCP	www > 45861 [ACK] Seq
20	16.732070	75.126.43.232	192.168.1.101	TCP	www > 45861 [ACK] Seq
21	18.072290	192.168.1.101	208.67.222.222	DNS	Standard query A www.
22	18.360176	208.67.222.222	192.168.1.101	DNS	Standard query response
23	18.445066	192.168.1.101	208.67.222.222	DNS	Standard query AAAA w
24	18.448504	192.168.1.101	208.67.222.222	DNS	Standard query A www.

Frame 1 (42 bytes on wire, 42 bytes captured)

Ethernet II, Src: D-Link 0a:f6:44 (00:17:9a:0a:f6:44), Dst: Cisco-Li 6a:c6:8b (00:18:39:6a:c6:8b)

000 00 18 39 6a c6 8b 00 17 9a 0a f6 44 08 06 00 01 ...9j....D....

010 08 00 06 04 00 01 00 17 9a 0a f6 44 c0 a8 01 65D...e

020 00 00 00 00 00 00 c0 a8 01 01D....

ame (frame), 42 bytes P: 582 D: 582 M: 0 Drops: 0

Capturing from Microsoft: \Device\NPF_{A9559F22-1504-4F4D-8067-DC61681A9F9C} [Wireshark 1.8.2 (SVN R...]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 5 Expression... Clear Apply Save >>

No.	Time	Source	Destination	Protocol	Length	Info
58	20.6015100	192.168.1.8	61.155.169.116	TCP	66	foliocorp > http [SYN] Seq=0 win=8192
59	20.6197360	61.155.169.116	192.168.1.8	TCP	66	http > foliocorp [SYN, ACK] Seq=0 Ack=1
60	20.6199200	192.168.1.8	61.155.169.116	TCP	54	foliocorp > http [ACK] Seq=1 Ack=1
61	20.6244780	192.168.1.8	61.155.169.116	HTTP	948	GET /tankxiao HTTP/1.1

Frame 58: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: Prodrive_26:12:bf (00:0f:11:26:12:bf), Dst: HuaweiDe_65:bc:c6 (54:a5:1b:65:bc:c6)

Internet Protocol Version 4, Src: 192.168.1.8 (192.168.1.8), Dst: 61.155.169.116 (61.155.169.116)

Transmission Control Protocol, Src Port: foliocorp (2242), Dst Port: http (80), Seq: 0, Len: 0

Source port: foliocorp (2242)

Destination port: http (80)

[Stream index: 5]

Sequence number: 0 (relative sequence number)

Header length: 32 bytes

Flags: 0x002 (SYN)

Window size value: 8192

[Calculated window size: 8192]

Checksum: 0x4bae [validation disabled]

Options: (12 bytes), Maximum segment size, No-Operation (NOP), window scale, No-Operation (NOP)

TCP第一次握手

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

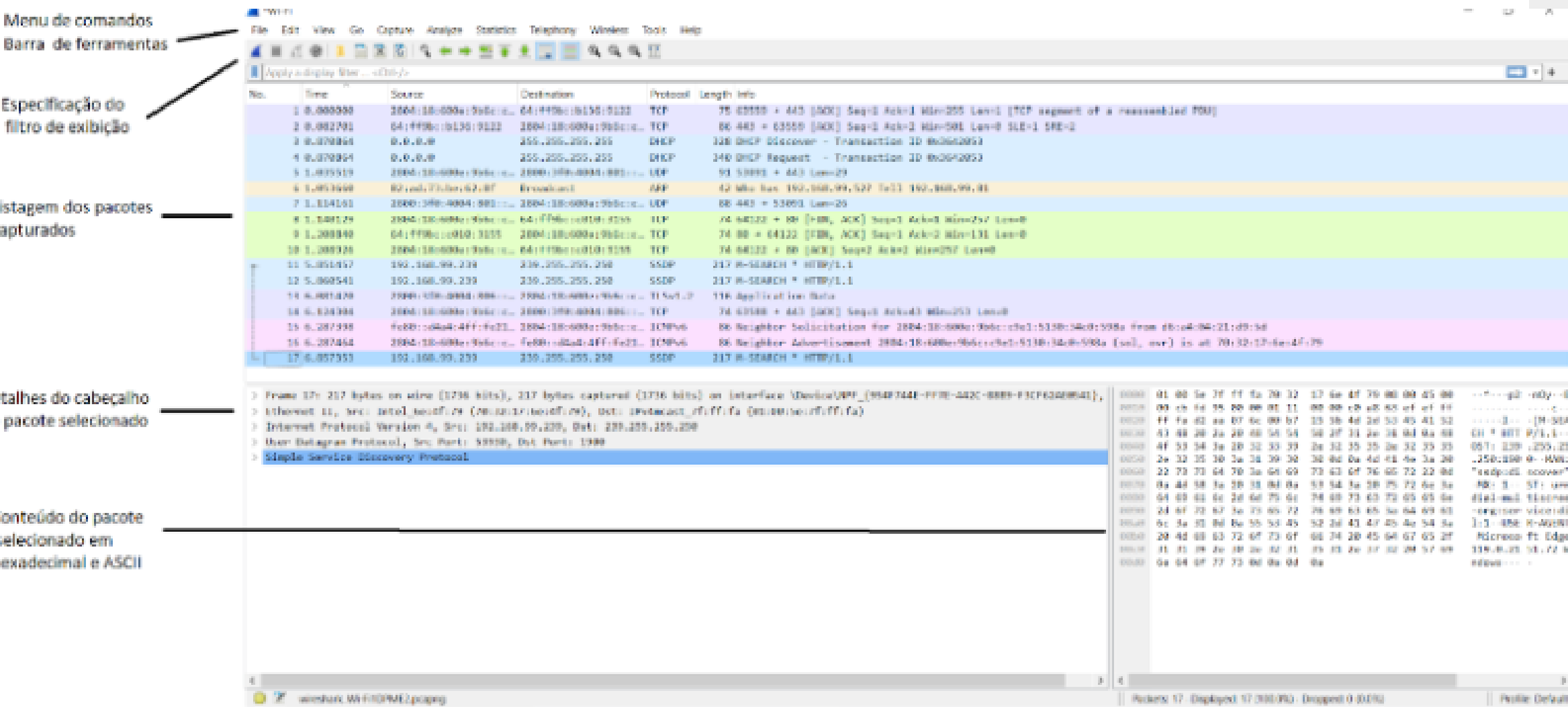
Capturas

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, detectação 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