Instituto Federal de Educação, Ciência e Tecnologia

Departamento de Telemática

Curso Tecnólogo em Telemática

Disciplina(s): Sistemas de Comunicação

Discente(s)/Matrícula: Jhonatan Silva de Sousa (20222013020032)

Carla Beatriz da Silva Teixeira (20211013020207)

Francisco Klayrton Vasconcelos da Silva (20079176857)

Docente: Márcio Caldas

Tema: Wireshark

Fortaleza – CE

2023

ÍNDICE

1. O que é Wireshark

Wireshark é um analisador de protocolo de rede criado por Gerald Combs em 1998. Ele 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.

Ele é executado na maioria das plataformas de computação, incluindo Windows, macOS, Linux e UNIX. Profissionais de rede, especialistas em segurança, desenvolvedores e educadores de todo o mundo o utilizam regularmente.

Está disponível gratuitamente como código aberto e é lançado sob a GNU General Public License versão 2.

É desenvolvido e mantido por uma equipe global de especialistas em protocolo e é um exemplo de tecnologia disruptiva.

O Wireshark inicialmente era conhecido como Ethereal, devido a problemas de marca registrada, em 2006 o projeto teve que ser renomeado.

2. Características do Wireshark

Dentre suas diversas funções suas principais características são:

- Inspeção profunda de centenas de protocolos
- Captura ao vivo e análise offline.
- Navegador de pacotes padrão de três painéis.
- Multiplataforma: roda em Windows, Linux, OS X, FreeBSD, NetBSD e muitos outros.
- Os dados de rede capturados podem ser navegados através de uma GUI ou através do utilitário TShark no modo TTY.
- Os filtros de exibição mais poderosos do setor.
- Análise VoIP rica.
- Ler/gravar muitos formatos de arquivo de captura diferentes: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compactado e descompactado), Sniffer® Pro e NetXray®, Network Instruments Observer , NetScreen snoop, Novell LANalyzer,

RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek e muitos outros.

- Os arquivos de captura compactados com gzip podem ser descompactados instantaneamente.
- Os dados ao vivo podem ser lidos de Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI e outros (dependendo da sua plataforma).
- Suporte de descriptografia para muitos protocolos, incluindo IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP e WPA/WPA2.
- As regras de coloração podem ser aplicadas à lista de pacotes para uma análise rápida e intuitiva.
- A saída pode ser exportada para XML, PostScript®, CSV ou texto simples.

3. Como Funciona o Wireshark

O Wireshark é uma ferramenta de análise de pacotes e sniffer de rede, mesmo sendo uma ferramenta altamente técnica, o Wireshark não é tão complicado de usar apenas os conceitos envolvidos no processo são voltados para pessoas com conhecimentos profundos de redes. Uma das principais funções dele é a 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.

O Wireshark permite filtrar o log antes do início da captura ou durante a análise. Assim, você pode afunilar e focar aquilo que procura no rastreamento da rede. Por exemplo, é possível definir um filtro para monitorar o tráfego em rede TCP entre dois endereços IP. Você pode configurar o filtro para mostrar apenas os pacotes enviados de um computador. Os filtros no Wireshark são um dos principais motivos que fizeram dele a ferramenta padrão para análise de pacotes.

Por padrão, o Wireshark captura apenas pacotes com destino ao ou origem no computador onde está sendo executado. Quando você selecionar "run Wireshark in

Promiscuous Mode" nas configurações de captura, é possível capturar a maior parte do tráfego na rede local (LAN).

Há muitos tutoriais e vídeos que ensinam como usar o Wireshark para fins específicos. Seu ponto de partida deve ser o site do Wireshark. Lá, você encontrará a documentação oficial do programa e uma página colaborativa no modelo Wiki.

Embora o Wireshark seja uma ótima ferramenta de análise e sniffer de rede, é mais bem utilizado, quando você sabe o que está procurando. Você não vai usar o Wireshark para encontrar um novo problema por conter muito ruído na rede.

4. Tipos de dados que podem ser capturados

O Wireshark é um analisador de pacotes de rede que permite aos usuários capturar e analisar o tráfego de rede em tempo real. Ele suporta uma ampla variedade de protocolos de rede, incluindo TCP, UDP, HTTP, DNS, MTP, POP3, e outros. A captura de dados da rede ocorre usando uma interface de rede em modo de "escuta", recebendo todos os pacotes pela interface de rede, independentemente de serem destinados ao host ou não e o tipo de conexão.

O programa decodifica os pacotes capturados e exibe para o usuário através de uma interface simples e amigável. Através de gráficos e filtros, o usuário pode visualizar dados referentes a protocolos, aplicações e dados de diagnósticos.

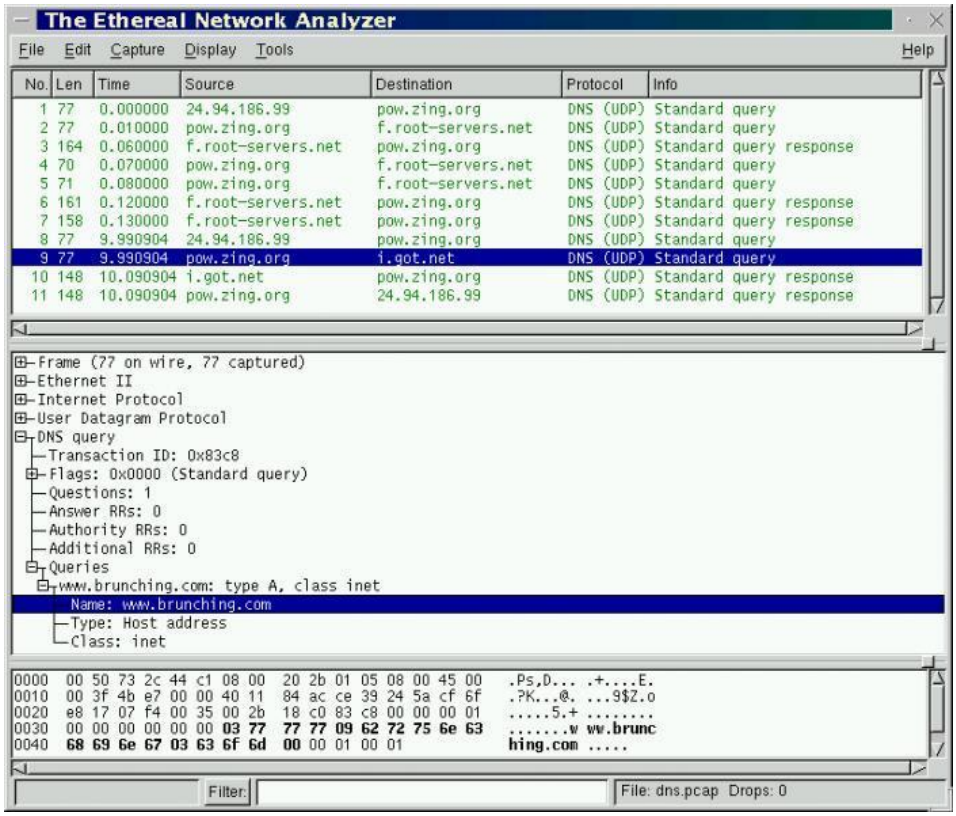
Os tipos de dados que podem ser capturados pelo Wireshark variam entre:

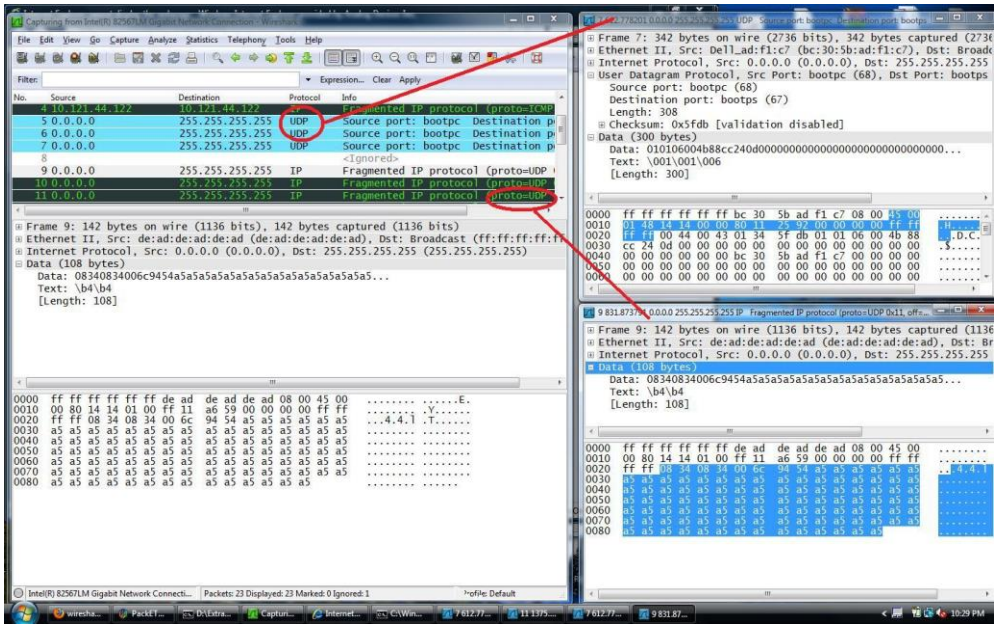
- Dados de protocolo: O Wireshark captura os dados brutos de protocolos, incluindo o cabeçalho do pacote e a carga útil. Esses dados de protocolo são valiosos para compreender a mecânica dos protocolos de rede, bem como para compreender os dados que são transferidos pela rede. Entre os protocolos capturados temos o ARP e ICMP, que servem para identificar rotas e endereçamento.
- 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, bem como para monitorar o uso da rede. Como o FTP para transferência de arquivos e IMAP para e-mails.

- Dados de diagnósticos: 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.

5. Ferramentas de análise do Wireshark

- Ferramenta de captura dos pacotes: permite que o usuário consiga visualizar todo o tráfego de determinada rede em tempo real e captar os picos de consumo;
- Filtragem: permite que o usuário consiga focar sua análise em pacotes específicos que estão circulando em determinada rede, baseando-se no endereço IP e protocolamento;
- Agrupamento: permite que sejam agrupados pacotes que possuem um fluxo específico;
- 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;
- Análise de Protocolos: função que permite que seja feita uma análise detalhada de diversos protocolos;
- Decodificação dos Pacotes: os pacotes capturados são decodificados permitindo que se obtenha informações detalhadas de cada pacote e seus protocolos.


The Ethereal Network Analyzer
File Edit Capture Display Tools Help
No. Len Time Source Destination Protocol Info
1 77 0.000000 24.94.186.99 pow.zing.org DNS (UDP) Standard query
2 77 0.010000 pow.zing.org f.root-servers.net DNS (UDP) Standard query
3 164 0.060000 f.root-servers.net pow.zing.org DNS (UDP) Standard query response
4 70 0.070000 pow.zing.org f.root-servers.net DNS (UDP) Standard query
5 71 0.080000 pow.zing.org f.root-servers.net DNS (UDP) Standard query
6 161 0.120000 f.root-servers.net pow.zing.org DNS (UDP) Standard query response
7 158 0.130000 f.root-servers.net pow.zing.org DNS (UDP) Standard query response
8 77 9.990904 24.94.186.99 pow.zing.org DNS (UDP) Standard query
9 77 9.990904 pow.zing.org i.got.net DNS (UDP) Standard query
10 148 10.090904 i.got.net pow.zing.org DNS (UDP) Standard query response
11 148 10.090904 pow.zing.org 24.94.186.99 DNS (UDP) Standard query response
Frame (77 on wire, 77 captured)
Ethernet II
Internet Protocol
User Datagram Protocol
DNS query
Transaction ID: 0x83c8
Flags: 0x0000 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.brunching.com: type A, class inet
Name: www.brunching.com
Type: Host address
Class: inet
0000 00 50 73 2c 44 c1 08 00 20 2b 01 05 08 00 45 00 .Ps,D... .+....E.
0010 00 3f 4b e7 00 00 40 11 84 ac ce 39 24 5a cf 6f .?K...@. ...9$Z.o
0020 e8 17 07 f4 00 35 00 2b 18 c0 83 c8 00 00 00 01 .....5.+ ....
0030 00 00 00 00 00 00 03 77 77 77 09 62 72 75 6e 63 ....w ww.brunc
0040 68 69 6e 67 03 63 6f 6d 00 00 01 00 01 hing.com .....
Filter:
File: dns.pcap Drops: 0


Frame 9: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits)
Ethernet II, Src: de:ad:de:ad:de:ad (de:ad:de:ad:de:ad), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
Data (108 bytes)
Data: 08340834006c9454a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5...
Text: \b4\b4
[Length: 108]
Frame 7: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: Dell_ad:f1:c7 (bc:30:5b:ad:f1:c7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Source port: bootpc (68)
Destination port: bootps (67)
Length: 308
Checksum: 0x5fdb [validation disabled]
Data (300 bytes)
Data: 010106004b88cc240d0000000000000000000000000000000...
Text: \001\001\006
[Length: 300]

6. Tipos de busca e filtragens

- Por IP origem/destino: possível fazer a filtragem dos pacotes através do IP de origem e destino da rota do pacote, utilizando ip.src==192.168.1.10 (origem) ip.dst==192.168.12.6 (destino)

- Por 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. Para esse caso, é necessário utilizar ip.src==192.168.0.0/24 and ip.dst==192.168.0.0/24

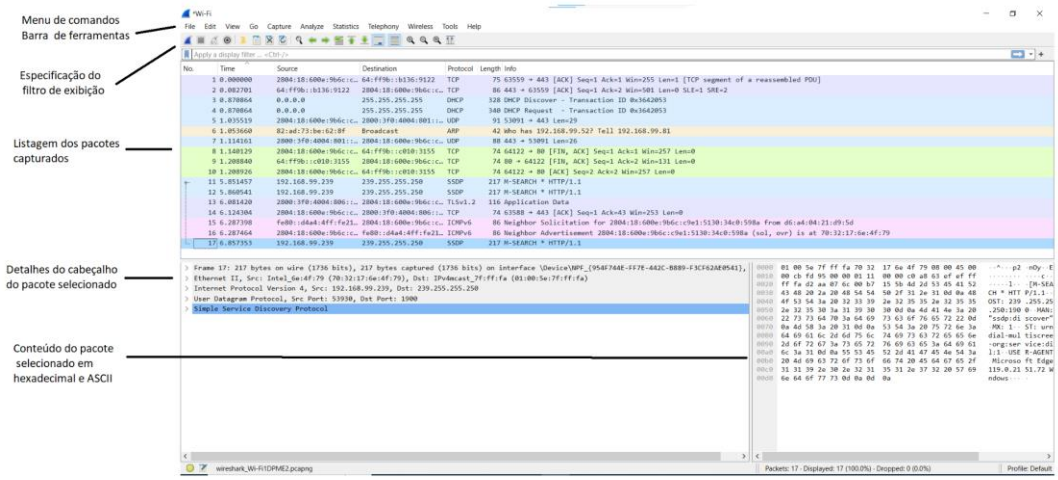
- Pelas portas TCP ou UDP: possível fazer essa filtragem de pacotes usando como referência a porta que está sendo utilizada na transação dos pacotes enviados. Nesse caso, é necessário utilizar tcp.port==350, udp.port==4357

- Através de BD MySQL/MariaDB: possível filtrar e monitorar o tráfego através das portas correspondentes ao servidor que hospeda o BD, sendo necessário utilizar tcp.port==50 || tcp.port==3109

7. Capturas realizadas Pelo Wireshark

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. Isso é chamado de espelhamento de porta ou SPAN. Quando é configurado para SPAN, ele envia uma cópia de todos os quadros para a porta SPAN. O Wireshark pode ser configurado para capturar pacotes da porta SPAN.

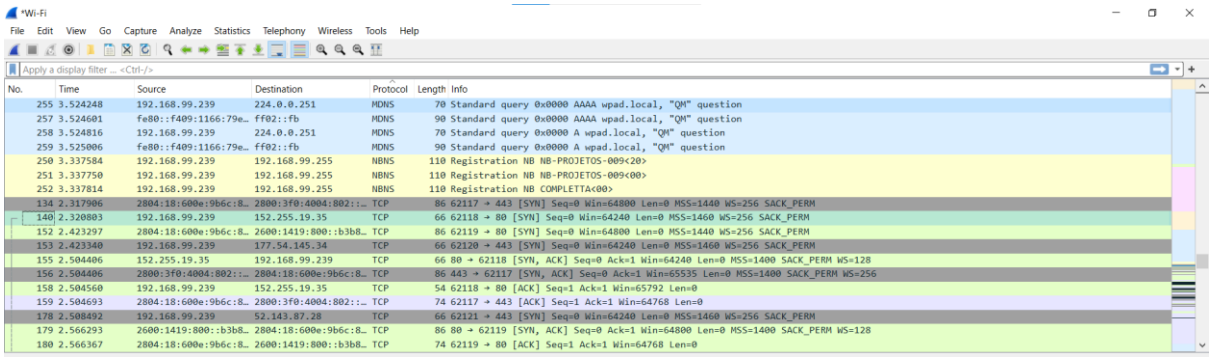
Agora iremos demonstrar uma captura feita pelo analisador. O ambiente utilizado foi uma máquina com o Windows 11 de uso pessoal, conectada a um modem roteador.

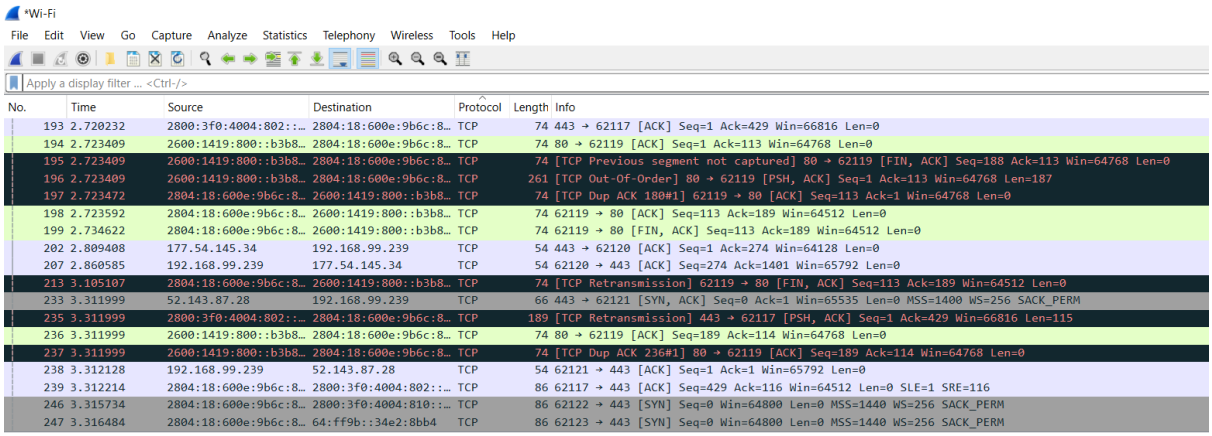


Ao iniciar a captura, podemos ver que a máquina realizou várias requisições, como buscas de endereços utilizando o protocolo ARP, pedido de um endereço IP utilizando protocolo DHCP, transferência de arquivos com o protocolo UDP e ICMP para informar erros de transmissão de dados.

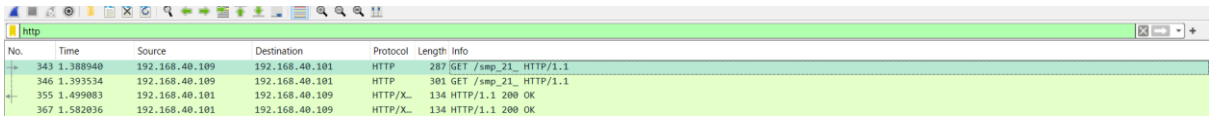
Observando o campo “listagem de pacotes”, temos um cabeçalho do programa onde podemos organizar os pacotes por time(tempo), origem(source), destination(destinatário), protocol(protocolo) , length(comprimento do pacote) e info(descrição). Além de organizar pelo cabeçalho do programa podemos ter uma visualização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

Nas capturas de tela abaixo podemos ver a organização por tipo de protocolo



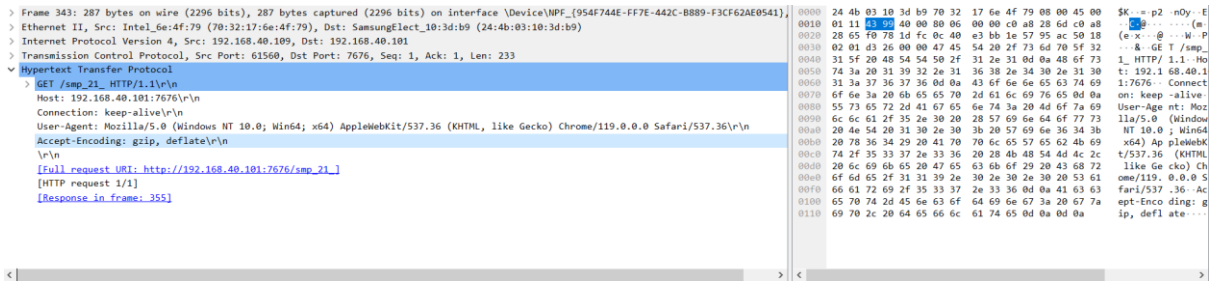


Agora vamos aplicar uma especificação de filtro para filtrar pacotes que utilizem o protocolo HTTP. no ambiente de teste é possível ver a troca de protocolos da máquina (com o IP 192.168.40.109, obtido por DHCP) em que o wireshark está rodando e uma TV da samsung (de IP 192.168.101).



Observando o canto esquerdo da imagem acima, podemos ver que o Wireshark indica o envio de algumas solicitações e o recebimento através de setas.

Além de informações básicas como a origem e destino, o Wireshark é capaz de realizar o desencapsulamento de alguns pacotes e obter o conteúdo presente no pacote. Como o HTTP é um protocolo simples que carrega texto, podemos verificar o conteúdo analisando apenas selecionando o pacote HTTP e depois na seção “Hypertext Transfer Protocol”.



Essas são algumas das várias análises que o programa pode realizar.

8. Usabilidade do programa Wireshark no mercado:

- Redes e Segurança: comumente 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;
- 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;
- Educação: na área de ensino o programa é normalmente utilizado pelos professores para demonstrar os temas teóricos abordados em sala e permitir que os alunos tenham acesso à prática do que está sendo proposto em aula;
- 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.

9. Conclusão

O objetivo inicial deste trabalho era fazer uma análise completa do programa Wireshark e suas ferramentas, entendendo onde cada ferramenta poderia ser utilizada e em quais áreas a usabilidade das funções seriam úteis.

Após o estudo apresentado neste trabalho percebe-se que a ferramenta é eficaz e auxilia em diversas áreas, principalmente a de TI, tornando o monitoramento e previsão de falhas em redes mais fácil e visual, através de seus parâmetros de medição e gráficos de análise dos resultados capturados.

Visto isso, considera-se que o programa Wireshark é de fato muito bom para tais análises e que a motivação do seu grande fluxo de uso é compatível com os benefícios que a ferramenta apresenta ao seu usuário final, deixando notória a veracidade do estudo desse trabalho e todos os aspectos ressaltados no mesmo.

10. Referências

BRITO, Edvaldo. **Como usar o Wireshark**. Techtudo.com.br, 2012. Disponível em: https://www.techtudo.com.br/noticias/2012/09/como-usar-o-wireshark.ghtml. Acesso em: 15/11/2023.

BUCKBEE, Michael. **Como usar o Wireshark: tutorial completo e dicas.** Varonis.com, 2022. Disponível em:https://www.varonis.com/pt-br/blog/how-to-use-wireshark#:~:text=O%20Wireshark%20permite%20filtrar%20o,TCP%20entre%20dois%20endereços%20IP. Acesso em: 15/11/2023.

Sobre o Wireshark.Wireshark.org, Disponível em: https://www.wireshark.org/about.html. Acesso em: 15/11/2023.

Wireshark Perguntas Frequentes. Wireshark.org. Disponível em: https://www.wireshark.org/faq.html#wheretogethelp. Acesso em: 15/11/2023.