



FACULDADE ANHANGUERA

TECNÓLOGO CIBERSEGURANÇA

NOME:TASSIANA MILKA FONTANA SOARES

ROTERIO DE AULA PRÁTICA

CAMPINAS-SP

2025

NOME:TASSIANA MILKA FONTANA SOARES

ROTERIO DE AULA PRÁTICA

Relatório da aula prática sobre análise de pacotes da rede utilizando o Wireshark.

CAMPINAS-SP

2025

SUMÁRIO

1.Introdução	4
2.Objetivos	4
3.Métodos	4
3.1. Quantidade de Pacotes	4
3.2. Protocolo dos Pacotes	5
3.2.1. TCP	5
3.2.2. TLSv1.2.....	5
3.2.3. UPD	5
3.2.4. ARP.....	6
3.2.5. DNS	6
3.2.6. QUIC.....	6
3.2.7. ICMPv6.....	6
3.3. Primeiro Pacote Identificado	7
3.4. Demonstração.....	7
4.Resolução	7
5.Conclusão	8
6. Referências Bibliográficas	8

1.Introdução

Em 1949 foi criado o primeiro software pelo cientista da computação Maurice Wilkes que é considerado por muitos como o nascimento do software moderno. Desde esse acontecimento conteve outros softwares reconhecidos.

Nessa sequência a utilização dos softwares começaram a estabilizar pelo mercado e aos usuários que trouxe suas vantagens e desvantagens de invasores aproveitarem e aplicarem vírus, pelo aplicativo falso o ataque dos dados ou rede.

Obteve a necessidade de criar segurança engenharia de softwares que são normas na finalidade de mais segurança dos aplicativos e reconhecer o que está incorreto pelos análise de ferramentas como Wireshark que para analisar uma varredura em rede de comunicação Local Area Network (LAN).

2.Objetivos

O objetivo principal é a utilidade do software aplicativo Wireshark analisar uma rede para descrever sobre o requisito desejado.

3.Métodos

- Todas as etapas sobre o análise de uma rede vai está em ordem desde da quantidade e protocolos do pacote encontrado.

3.1. Quantidade de Pacotes

- Durante o análise observa-se mais de 100 pacotes localizados na rede Wi-fi de diferentes numerações, tempo de execução e o destino sobre porta da entrada ou saída.

3.2. Protocolo dos Pacotes

- Pela análise foi encontrado vários protocolos conforme nas descrições a abaixo:

3.2.1. TCP

- Protocolo de Controle de Transmissão que é uma comunicação de camada para transporte da rede dos computadores do Modelo OSI que é o suporte a rede Internet dos dados enviados na sequência e reconhecido como TCP/IP de nós da rede;

3.2.2. TLSv1.2

- TLSv1.2 é reconhecido como protocolo de segurança que transfere dados do cliente em servidor no formato de criptografia;

3.2.3. UPD

- Um protocolo que permite transmissão de conexão do diagramas baseados em IP na velocidade de transmissão, segurança e integridade do funcionamento;

3.2.4. ARP

- Procedimento que conecta com endereço de protocolo de internet (IP) em constante mudança e chega em gateway a um endereço de máquina físico como endereço de controle o acesso da rede local (LAN);

3.2.5. DNS

- Interação de endereço do protocolo de internet (IP) com os nomes de domínio em endereços para navegadores que possa carregar os recursos da internet e acessar informações on-line por meio de nomes de domínio;

3.2.6. QUIC

- Um protocolo de rede de camada para propósitos gerais com mais da metade de todas as conexões do navegador com multiplexadas do HTTP/2 que permite múltiplos fluxos de dados que cheguem a todos os pontos terminais de forma independente que envolva outros fluxos da transmissão dos protocolos;

3.2.7. ICMPv6

- Uma versão nova de protocolo definido pela RFC 4443 que precisa de suporte completo para implementar IPV6.

3.3. Primeiro Pacote Identificado

- O primeiro pacote identificado foi o TCP com tempo de 1 0.000000 e destino 192.168.1.3.

3.4. Demonstração

- Na FIGURA 1 contém a demonstração sobre a descoberta dos protocolos, frame, ethernet, Internet Protocol e transmission control protocol.

FIGURA 1: Protocolos

The screenshot shows the Wireshark interface with a packet list on the left and a packet details pane on the right. The packet list shows 18 packets, with the first packet (Frame 1) selected. The packet details pane shows the structure of the first packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	20.49.150.241	192.168.1.3	TCP	1494	443 → 49920 [ACK] Seq=1 Ack=1 Win=16384 Len=1440 [TCP PDU reassembled in 3]
2	0.000000	20.49.150.241	192.168.1.3	TCP	1494	443 → 49920 [ACK] Seq=1441 Ack=1 Win=16384 Len=1440 [TCP PDU reassembled in 3]
3	0.000000	20.49.150.241	192.168.1.3	TLSv1.2	932	Server Hello, Certificate, Server Key Exchange, Server Hello Done
4	0.000093	192.168.1.3	20.49.150.241	TCP	54	49920 → 443 [ACK] Seq=1 Ack=3759 Win=255 Len=0
5	0.005292	192.168.1.3	20.49.150.241	TLSv1.2	232	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
6	0.188148	20.49.150.241	192.168.1.3	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
7	0.188148	20.49.150.241	192.168.1.3	TLSv1.2	123	Application Data
8	0.188266	192.168.1.3	20.49.150.241	TCP	54	49920 → 443 [ACK] Seq=159 Ack=3879 Win=255 Len=0
9	0.194590	192.168.1.3	20.49.150.241	TLSv1.2	141	Application Data
10	0.194767	192.168.1.3	20.49.150.241	TLSv1.2	1066	Application Data
11	0.194943	192.168.1.3	20.49.150.241	TLSv1.2	92	Application Data
12	0.378886	20.49.150.241	192.168.1.3	TCP	54	443 → 49920 [ACK] Seq=3879 Ack=1296 Win=16385 Len=0
13	0.378886	20.49.150.241	192.168.1.3	TLSv1.2	92	Application Data
14	0.425999	192.168.1.3	20.49.150.241	TCP	54	49920 → 443 [ACK] Seq=1296 Ack=3917 Win=255 Len=0
15	0.607113	20.49.150.241	192.168.1.3	TLSv1.2	409	Application Data
16	0.611152	192.168.1.3	20.49.150.241	TCP	54	49920 → 443 [FIN, ACK] Seq=1296 Ack=4272 Win=253 Len=0
17	0.746212	192.168.1.3	20.49.150.241	TCP	66	49921 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
18	0.794859	20.49.150.241	192.168.1.3	TLSv1.2	96	Application Data

Frame 1: 1494 bytes on wire (11952 bits) on interface \Device\NPF_{EBADEB2-5B7E-4589-83CA-2B07DFE85C5C}, id 0
 Ethernet II, Src: GongjinElect_26:e1:b0 (ec:b3:13:26:e1:b0), Dst: LiteonTechno_c3:a6:43 (c0:35:32:c3:a6:43)
 Internet Protocol Version 4, Src: 20.49.150.241, Dst: 192.168.1.3
 Transmission Control Protocol, Src Port: 443, Dst Port: 49920, Seq: 1, Ack: 1, Len: 1440

Fonte: autoria própria

4. Resolução

Durante a realização obtive o entendimento sobre o começo dos softwares, análise da ferramenta para saber o andamento de uma rede doméstica de wi-fi a demonstração dos protocolos encontrados em tempo real de minutos que definindo os principais pontos como a entrada e saída.

5. Conclusão

Conforme descrito o software surgiu em 1949 pelo Maurice Wilkes que conteve a necessidade da criação de segurança para manter mais estável os dados dos usuários na utilização dos aplicativos juntamente na conexão com uma rede para visualizar o acesso.

6. Referências Bibliográficas

SOFTWAREPOLITICO.Qual foi o primeiro software criado? - Software Político. Disponível em:<https://softwarepolitico.com.br/noticias/qual-foi-o-primeiro-software-criado/> .Acesso em:11/04/2025.

CISCE.Segurança em Desenvolvimento de Software.Disponível em:<https://cisce.com.br/blog/seguranca-em-desenvolvimento-de-software/> .Acesso em:11/04/2025.

WIKIPÉDIA.Protocolo de Controle de Transmissão – Wikipédia, a enciclopédia livre. Disponível em:https://pt.wikipedia.org/wiki/Protocolo_de_Controlde_de_Transmiss%C3%A3o .Acesso em:11/04/2025.

GIGAMON. O que é TLS 1.2? - Gigamon Blog.Disponível em:<https://blog.gigamon.com/2021/07/14/what-is-tls-1-2-and-why-should-you-still-care/#:~:text=Transport%20Layer%20Security%20%28TLS%29%201.2%20is%20a%20security,data%20that%E2%80%99s%20transmitted%20between%20a%20client%20and%20server> . Acesso em:11/04/2025.

IONOS.UDP: O que é UDP?-IONOS MX.Disponível em:<https://www.ionos.mx/digitalguide/servidores/know-how/udp-user-datagram-protocol/> .Acesso em:11/04/2025.

CLOUDFLARE. O que significa DNS e como a internet funciona | Cloudflare.Disponível em:<https://www.cloudflare.com/pt-br/learning/dns/what-is-dns/> .Acesso em:11/04/2025.

WIKIPÉDIA.QUIC – Wikipédia, a enciclopédia livre.Disponível em:<https://pt.wikipedia.org/wiki/QUIC> .Acesso em:11/04/2025.

WIKIPÉDIA.ICMPv6 – Wikipédia, a enciclopédia livre.Disponível em:<https://pt.wikipedia.org/wiki/ICMPv6>.Acesso em:11/04/2025.