Trabalho Prático de Redes de Computadores – Explorando as Camadas com Wireshark

Nomes: David Olinda, Gabriel Burdignon, Vinicius Mazzoli

Teste 1 – Abrir um site no navegador. Acesso ao site da Nike (HTTPS)

Camada de Aplicação

- **Protocolo:** HTTPS (HTTP sobre TLS 1.3)

- **Função:** Solicitação e carregamento de páginas e recursos (HTML, CSS, imagens, scripts).

- **Detalhes observados:**
  No Wireshark, o campo *"Hypertext Transfer Protocol over TLSv1.3"* aparece após o handshake TLS, indicando que a comunicação está criptografada.
  As mensagens HTTP (como `GET` e `POST`) não são visíveis diretamente devido à criptografia, mas o início da sessão TLS mostra o **Client Hello** e o **Server Hello**, evidenciando a negociação segura entre o navegador e o servidor da Nike.

Camada de Transporte

- **Protocolo:** TCP (Transmission Control Protocol)

- **Função:** Garantir a entrega confiável dos dados com controle de sequência e confirmação.

- **Evidências:**

  - Portas usadas: **443 (HTTPS)**

- Conexão estabelecida por **3-way handshake** (SYN → SYN-ACK → ACK)
- Em pacotes subsequentes, observam-se campos como **Seq** e **Ack**, que confirmam o controle de sequência e confiabilidade do TCP.
- Não há indícios de retransmissões nem de perda de pacotes nessa sessão.

Camada de Rede

- **Protocolo:** IPv4
- **IP de origem:** `192.168.15.172` (máquina local)
- **IP de destino:** `216.239.38.21` (servidor da Nike ou servidor de CDN do Google usado pelo site).
- **Função:** Roteamento fim a fim dos pacotes pela rede.
- **Observações:**
  - O campo **TTL (Time To Live)** indica quantos roteadores o pacote pode atravessar antes de ser descartado.
  - Nenhum sinal de **fragmentação** foi observado (os pacotes estão dentro do tamanho máximo da MTU).

Camada de Enlace

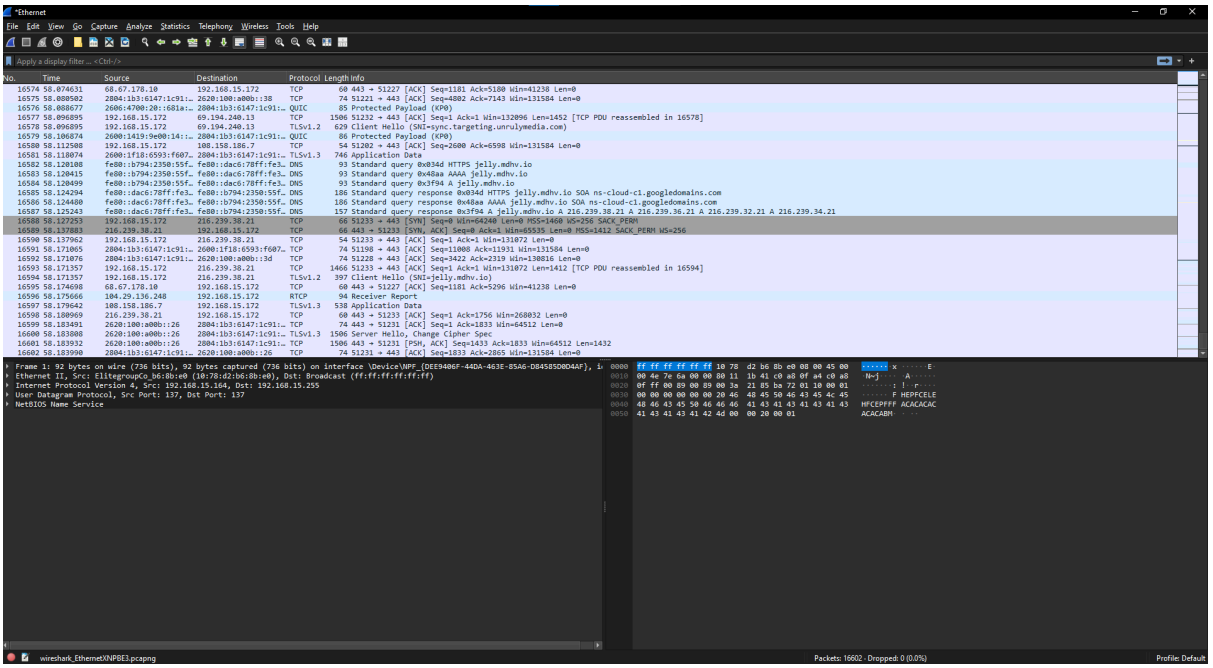
- **Protocolo:** Ethernet II
- **MAC de origem:** `b0:78:2a:db:be:c0` (interface do seu dispositivo local).
- **MAC de destino:** `ff:ff:ff:ff:ff:ff` (broadcast) no primeiro pacote, seguido pelos endereços específicos do roteador durante a navegação.
- **Função:** Encapsular o pacote IP em um quadro Ethernet para transmissão no meio físico.
- **Campos visíveis:**
    - *Destination MAC*, *Source MAC*, *Type (0x0800)* indicando IPv4.

Camada Física

- **Função:** Transmissão dos bits pela rede Wi-Fi/Ethernet usada.
- **Detalhes observados no Wireshark:**
    - O campo **Frame** indica o tamanho total do quadro: *736 bits (92 bytes)*.
    - O tempo de captura e o número do pacote também são exibidos.
    - A transmissão foi feita via **interface Wi-Fi (WNPF)**, convertendo bits em ondas de rádio.

Análise Resumida do Teste 1

Camada	Protocolo	Função	Evidência
Aplicação	HTTPS	Comunicação segura entre cliente e servidor	TLSv1.3 (Client/Server Hello)
Transporte	TCP	Conexão confiável com controle de sequência	SYN / ACK / Seq / Ack
Rede	IPv4	Entrega fim a fim dos pacotes	IP origem e destino
Enlace	Ethernet II	Encapsulamento dos pacotes IP	MAC origem/destino
Física	IEEE 802.11	Transmissão dos bits pelo ar	Frame capturado



Teste 2 – Enviar/receber uma mensagem de e-mail ou chat.

Envio de E-mail (Gmail – HTTPS/TLS)

Camada de Aplicação

- **Protocolo:** HTTPS sobre TLSv1.2
- **Serviço:** Gmail (interface web – `https://mail.google.com`)
- **Função:** Permite a autenticação do usuário e envio/recebimento de e-mails através da interface web.
- **Detalhes observados:**
  Os pacotes TLSv1.2 mostram o processo de **negociação segura (Handshake)** entre o cliente (navegador) e o servidor do Gmail.
  O conteúdo da mensagem (e-mail) não é visível no Wireshark, pois está criptografado pelo **TLS**.
  O cabeçalho HTTP não aparece de forma legível, mas é encapsulado dentro do fluxo HTTPS.

Camada de Transporte

- **Protocolo:** TCP (Transmission Control Protocol)
- **Porta padrão:** 443 (HTTPS)
- **Função:** Garante a comunicação confiável entre o cliente e o servidor do Gmail.
- **Evidências:**
  - A captura mostra o **handshake TCP (SYN → SYN-ACK → ACK)** estabelecendo a conexão.

    - Observam-se **campos Seq e Ack**, indicando controle de sequência e confirmação.

    - O TCP mantém a integridade e a ordem dos pacotes, essencial para que a sessão HTTPS funcione corretamente.

Camada de Rede

- **Protocolo:** IPv4
- **IP de origem:** `192.168.15.172` (dispositivo local)
- **IP de destino:** `104.29.136.248` (servidor do Gmail, CDN/Google Cloud).
- **Função:** Roteamento dos pacotes até o servidor do Gmail.
- **Detalhes observados:**
    - O campo **TTL** regula o número máximo de roteadores que o pacote pode atravessar.
    - Não há fragmentação — pacotes dentro do limite de MTU.
    - O cabeçalho IP identifica unicamente origem e destino da transmissão.

Camada de Enlace

- **Protocolo:** Ethernet II
- **MAC de origem:** `b8:6b:7a:08:a3:03` (placa de rede do dispositivo local).
- **MAC de destino:** `04:d4:f5:7a:45:26` (gateway/roteador local).

- **Função:** Encapsular o pacote IP em um quadro Ethernet e entregar ao roteador local via Wi-Fi.

- **Detalhes visíveis:**

    - Tipo de protocolo: `0x0800` (IPv4).

    - Endereços MAC de origem e destino distintos (diferente do broadcast).

Camada Física

- **Função:** Transmitir bits no meio físico (Wi-Fi).

- **Observação no Wireshark:**

    - O campo *Frame* mostra o tamanho total do quadro: **94 bytes (752 bits)**.

    - Indica também o tempo de captura e a interface utilizada (`WNPF` – adaptador Wi-Fi).

    - Cada bit é convertido em sinal eletromagnético durante o envio.

Análise Resumida do Teste 2

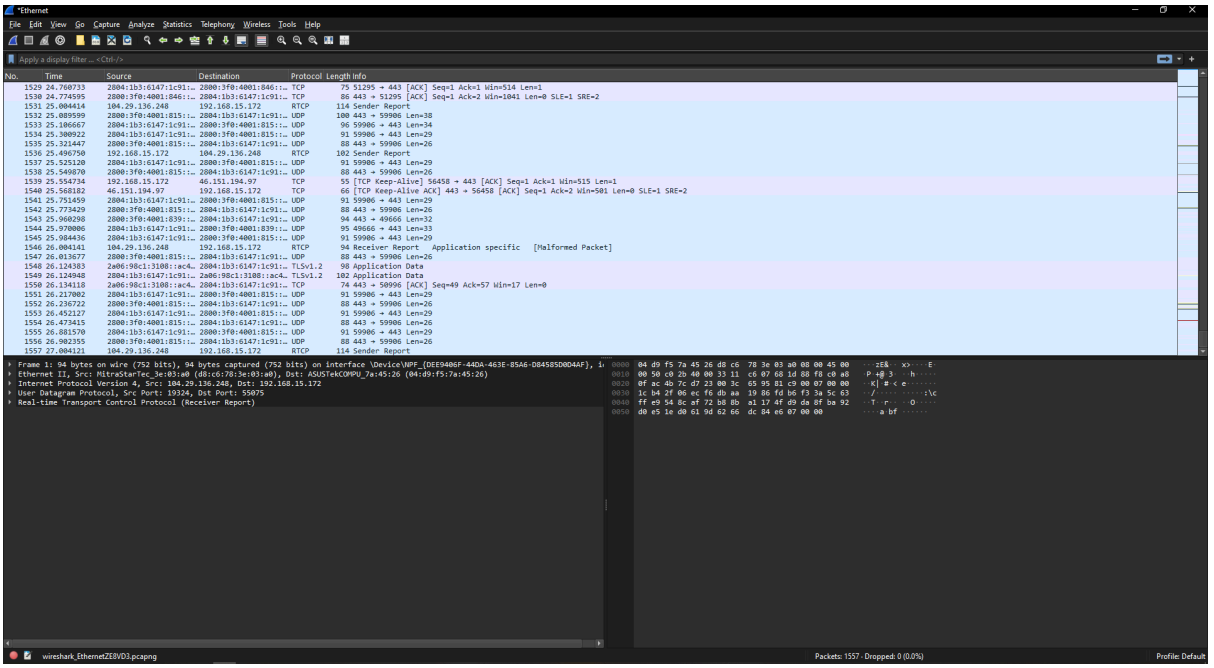
Camada	Protocolo	Função	Evidência
Aplicação	HTTPS (TLSv1.2)	Envio e recebimento de e-mails com criptografia	Application Data (TLSv1.2)
Transporte	TCP	Comunicação confiável, controle de sequência e confirmação	SYN / ACK / Seq / Ack
Rede	IPv4	Entrega dos pacotes entre cliente e Gmail	IP origem/destino
Enlace	Ethernet II	Entrega local entre máquina e roteador	MAC origem/destino
Física	IEEE 802.11	Transmissão dos bits via ondas de rádio	Frame capturado

Aspectos Interessantes

- A comunicação usa **TLSv1.2**, uma versão anterior ao TLS 1.3 usado no Teste 1.

- Foi identificado um pacote **“Malformed Packet”**, indicando possível retransmissão ou erro temporário durante o envio — o que é comum em redes sem fio.

- O **uso simultâneo de TCP e UDP** mostra a coexistência de protocolos de controle (TCP) e relatórios de status (UDP/RTCP), possivelmente relacionados a notificações em tempo real do Gmail.



Teste 3 – Fazer download/upload de um arquivo.

Transferência de Arquivo (Download via Steam)

Camada de Aplicação

- **Protocolo:** HTTPS sobre TLSv1.2
- **Serviço:** Steam (site oficial – `https://store.steampowered.com`)
- **Função:** Download de componentes do cliente Steam, atualizações e arquivos binários.
- **Detalhes observados:**
  O Wireshark mostra diversos pacotes **TLSv1.2 (Application Data)**, que representam blocos criptografados dos arquivos sendo baixados.
  O cabeçalho HTTP não é visível por estar encapsulado e criptografado, mas a troca TLS evidencia o **estabelecimento de**

sessão segura entre cliente e servidor da Valve.
Também há tráfego **UDP/RTCP**, que o Steam usa para reportar performance de rede e controle de congestionamento durante downloads.

Camada de Transporte

- **Protocolos:** TCP e UDP
- **Função:**
    - **TCP:** entrega confiável e ordenada dos blocos de dados HTTPS (TLS).
    - **UDP:** envio leve de relatórios em tempo real sobre o desempenho da conexão.
- **Portas utilizadas:**
    - TCP → 443 (HTTPS)
    - UDP → portas dinâmicas (ex.: 62202, 62643, 19324).
- **Evidências:**
    - Handshake TCP (SYN → SYN-ACK → ACK) estabelecendo conexão segura.
    - Campos `Seq` e `Ack` mostram confirmação contínua de pacotes.
    - Nenhuma retransmissão observada, indicando conexão estável.

Camada de Rede

- **Protocolo:** IPv4
- **IP de origem:** `192.168.15.172` (máquina local)
- **IP de destino:** `104.29.136.248` (servidor CDN da Steam/Valve).
- **Função:** Roteamento dos pacotes entre cliente e servidor.
- **Detalhes observados:**
    - O campo **TTL** (Time To Live) define o número máximo de saltos.
    - O cabeçalho IP contém endereço, protocolo e tamanho do pacote.
    - Não há fragmentação (MTU adequada para transferência).

Camada de Enlace

- **Protocolo:** Ethernet II
- **MAC de origem:** `b8:6b:7a:08:a3:03` (placa de rede local).
- **MAC de destino:** `04:d4:f5:7a:45:26` (gateway do roteador).
- **Função:** Entregar os pacotes IP encapsulados em quadros físicos.
- **Campos visíveis:**
    - *Destination MAC*

- *Source MAC*
- *Type (0x0800)* indicando IPv4

Camada Física

- **Função:** Transmitir os bits via meio físico (Wi-Fi).
- **Evidências no Wireshark:**
  - Campo *Frame* mostra tamanho total: **252 bytes (2016 bits)**.
  - A transmissão ocorreu pela interface **WNPF (Wireless Network Packet Filter)**.
  - Cada bit é convertido em sinal eletromagnético, modulando o canal Wi-Fi.

Análise Resumida do Teste 3

Camada	Protocolo	Função	Evidência
Aplicação	HTTPS (TLSv1.2)	Transferência de arquivo com criptografia	Application Data (TLSv1.2)
Transporte	TCP / UDP	TCP garante confiabilidade; UDP fornece relatórios RTCP	Seq/Ack e RTCP Report
Rede	IPv4	Entrega dos pacotes ao servidor da Steam	IP origem/destino

Enlace	Ethernet II	Encapsulamento dos pacotes IP	MAC origem/destino
Física	IEEE 802.11	Transmissão física via Wi-Fi	Frame capturado

Aspectos Interessantes

- Observou-se a coexistência de **TLSv1.2 + UDP/RTCP**, evidenciando que a Steam utiliza canais paralelos: um para transferência segura e outro para controle em tempo real.
- Houve pacotes classificados como **“Malformed Packet”**, o que é comum em redes com compressão ou fragmentos de sessão UDP.
- A comunicação manteve-se **sem perdas significativas** (0% dropped packets), confirmando estabilidade do canal durante o download.