

Informática Redes de computadores Laboratório Wireshark 1: introdução

30 de março de 2025

## Informações importantes

• Você pode instalar o pacote wireshark nos sistemas Linux ou baixar o Wireshark para Windows em https://www.wireshark.org/download.html.

O Wireshark é um *packet sniffer*, ou analisador de pacotes. Este programa consegue capturar os pacotes que são enviados ou recebidos pelo seu computador, de forma que você possa visualizar e analisar as mensagens trocadas. Os pacotes não são bloqueados, o Wireshark apenas copia os pacotes para que você possa analisá-lo; as mensagens continuam trafegando pela rede normalmente.

- 1. Inicie a captura no Wireshark, usando qualquer interface (any);
- Acesse a página Web http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html no seu navegador;
  - Tenha certeza que está acessando a página usando apenas HTTP, e não HTTPS, que é criptografado.
  - Você pode clicar no cadeado ao lado da URL para tentar desabilitar isso.
- 3. No Wireshark, você deve ver uma série de pacotes trafegando em seu computador. Perceba a quantidade de pacotes trafegando mesmo quando você só acessa uma página!;
- 4. Pare a captura. Agora vamos apenas inspecionar os pacotes que já foram trocados pela rede;
- 5. Digite http no filtro. Você deve ver poucos pacotes relacionados ao conteúdo da página acessada;
- 6. Explore as mensagens do tipo HTTP GET e HTTP OK para visualizar a requisição (ou o pedido) do seu navegador e a resposta com o conetúdo da página. Perceba que o mesmo conteúdo que o seu navegador mostrou aparece no pacote inspecionado;

## 1 Exercícios

- 1. Liste 3 outros protocolos que aparecem nas mensagens capturadas (lembre-se de remover o filtro HTTP);
- 2. Quanto tempo demorou entre o envio da mensagem HTTP GET e o recebimento da resposta HTTP OK? Você já encontrou os pacotes com a requisição e a resposta, calcule o tempo usando a coluna "Time";
- 3. Qual é o endereço IP do seu computador? E do servidor que contém a página acessada?