

Redes de Computadores

Prof. Giancarlo Michelino
Gaeta Lopes

Aula 4

Análise de tráfego de rede

Redes de computadores – Aula prática 4

Etapa 1

Monitoramento
de redes

Etapa 2

Análise de tráfego

Etapa 1

Redes cabeadas

Wireshark

- ▶ Através do Wireshark é possível controlar o tráfego de uma rede e monitorar a entrada e saída de dados do computador, em diferentes protocolos, ou da rede à qual o computador está ligado.
- ▶ Possibilidade de criar inúmeros filtros para visualizar os dados desejados.



Fonte: <https://www.wireshark.org/>

Wireshark

- ▶ Filtros para os dados:
 - ip.dst → endereço ip do destinatário;
 - ip.src → endereço ip de quem envia o pacote;
 - ip.addr → filtra todo o tráfego do endereço de ip;
 - icmp.type == 8 → comandos ICMP (ping).

Procedimento 1

- ▶ Identifique o ip do computador de um colega, conectado a uma mesma rede que você.
- ▶ Abra o Wireshark e crie um filtro para requisições de ping que chegam a sua máquina.
- ▶ Peça para o seu amigo enviar ping para sua máquina e vice-versa.
- ▶ Verifique se o endereço de IP dele aparece no Wireshark.

Etapa 2

Redes wifi

Hercules

- ▶ Terminal de porta serial, UDP e TCP (client/server).
- ▶ Disponível para download em https://www.hw-group.com/files/download/sw/version/hercules_3-2-8.exe.
- ▶ Permite o envio de dados por meio de uma conexão TCP entre dois computadores em uma mesma rede.



Fonte: <https://goo.gl/1jpQDo>.

Procedimento 2

- ▶ Abra o Hércules em dois computadores ligados na mesma rede.
- ▶ Crie uma conexão TCP entre os dois computadores, sendo um deles o servidor, em uma porta qualquer.
- ▶ Faça testes na conexão, enviando dados em ambos os computadores.
- ▶ Crie um filtro no Wireshark para a porta selecionada.
- ▶ Envie dados no Hércules e verifique se eles aparecem no Wireshark.