

# Prática com Wireshark

---

Prof. Ricardo José Pfitscher

Material baseado em:

[http://gaia.cs.umass.edu/wireshark-labs/Wireshark\\_Intro\\_v7.0.pdf](http://gaia.cs.umass.edu/wireshark-labs/Wireshark_Intro_v7.0.pdf)

# Introdução

1. Vamos realizar uma atividade prática com um *sniffer* de rede
2. O que é um *sniffer*?

# Introdução

1. Vamos realizar uma atividade prática com um *sniffer* de rede
2. O que é um *sniffer*?
  - a. Aplicativo de software que captura pacotes que são enviados e recebidos no seu computador;
  - b. Ele também armazena e/ou mostra os conteúdos e os múltiplos campos dos protocolos capturados;
  - c. Ele atua de forma **passiva**: ele não manda pacotes

# Packet sniffer

1. A *biblioteca de captura de pacotes* recebe uma cópia de cada frame do nível de enlace enviado e recebido do/pelo seu computador;
2. O *analisador de pacotes* que mostra todos os conteúdos das mensagens dos protocolos;

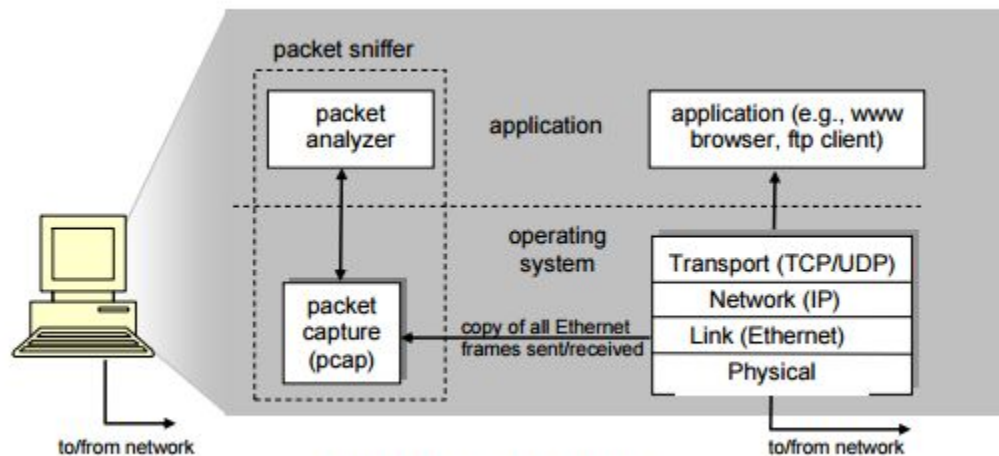


Figure 1: Packet sniffer structure

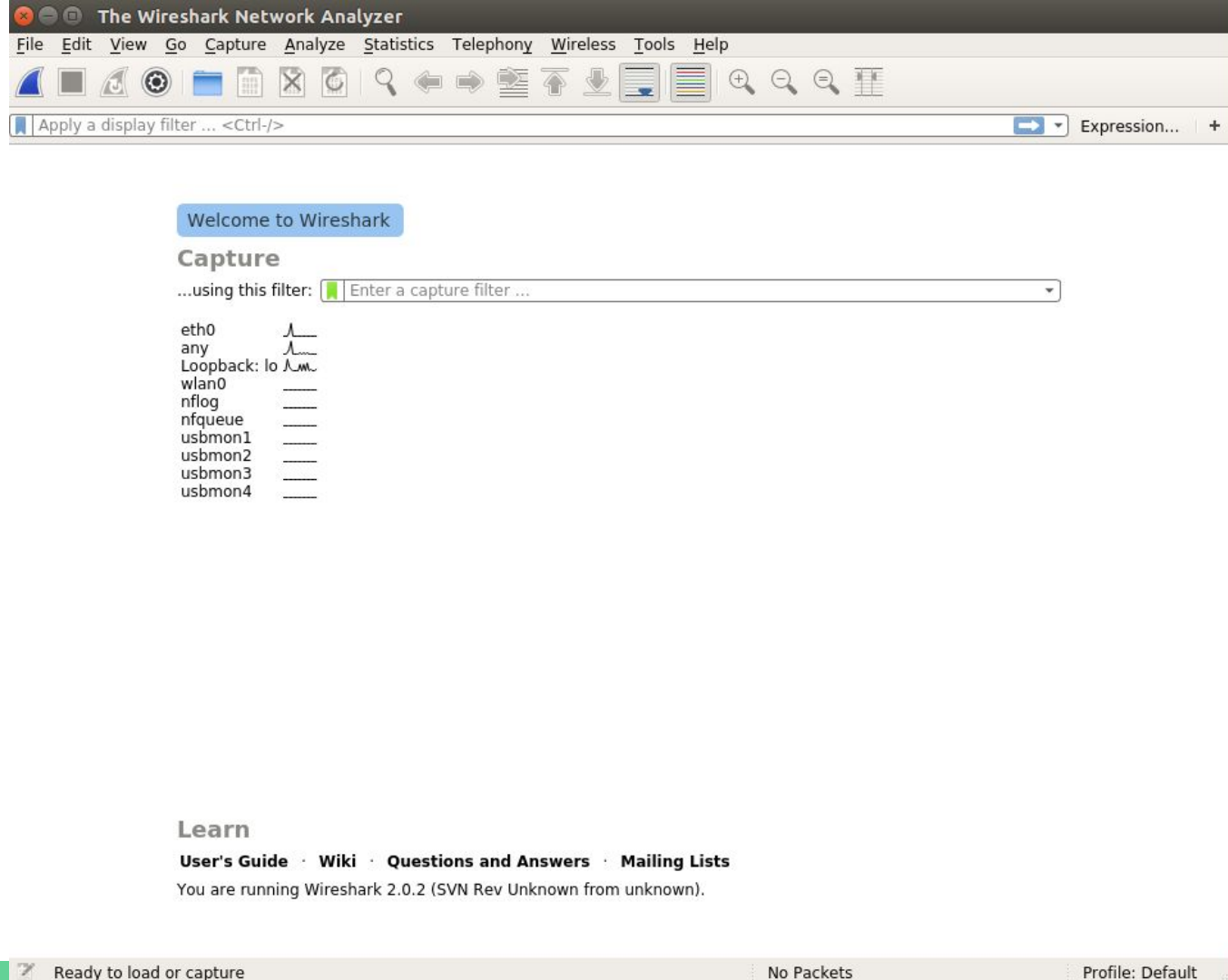
# Wireshark

1. Nessa disciplina vamos utilizar o wireshark para analisar o comportamento dos protocolos
  - a. <https://www.wireshark.org/>
  - b. Software gratuito e disponível para Windows, Linux e Mac
2. Faça o download e instale o aplicativo no seu computador
  - a. É preciso ter privilégios administrativos para Instalar/Executar
    - i. Durante a captura o Wireshark tem de colocar as interfaces em modo promíscuo
    - ii. O que é isso?
      1. Google Images: Promíscuo → Do not do that!
    - iii. Todos os pacotes que trafegam no segmento são capturados pelo receptor, e não somente os endereçados a ele

# Wireshark

## 1. Tela inicial

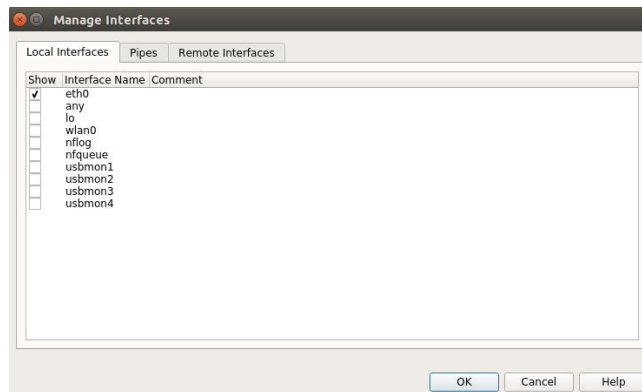
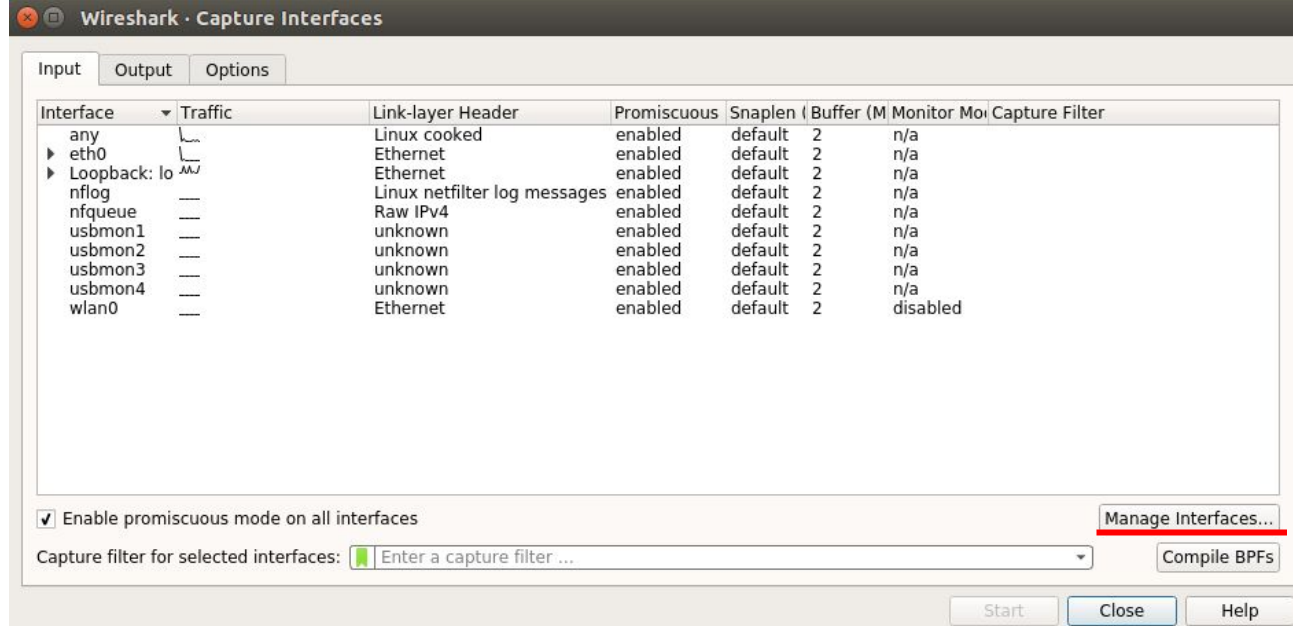
- Nada demais...
- Configure as interfaces clicando no settings



# Wireshark

## 1. Tela inicial

- Nada demais...
- Configure as interfaces clicando no settings
- Ou
- Dois cliques na interface de interesse (eth0)



# Wireshark

## 1. Tela de Captura

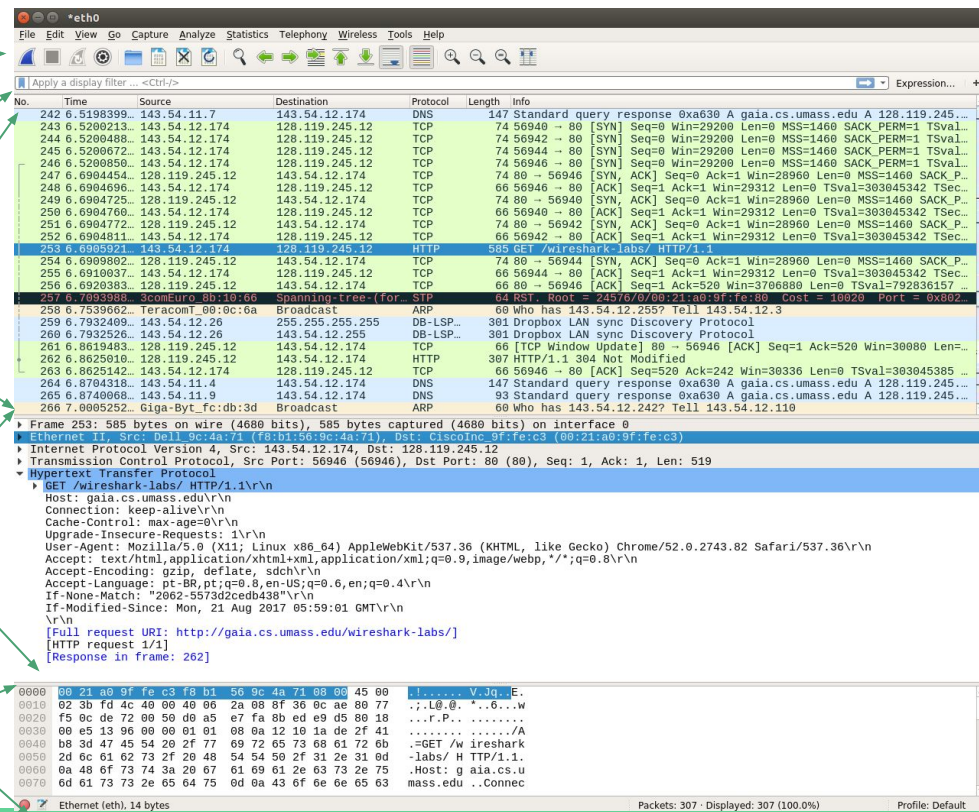
Menus de comando

Especificação de filtros

Lista de pacotes capturados


Detalhes do pacote selecionado

Conteúdo do pacote em hexadecimal e ASCII





# Primeira captura [1/2]

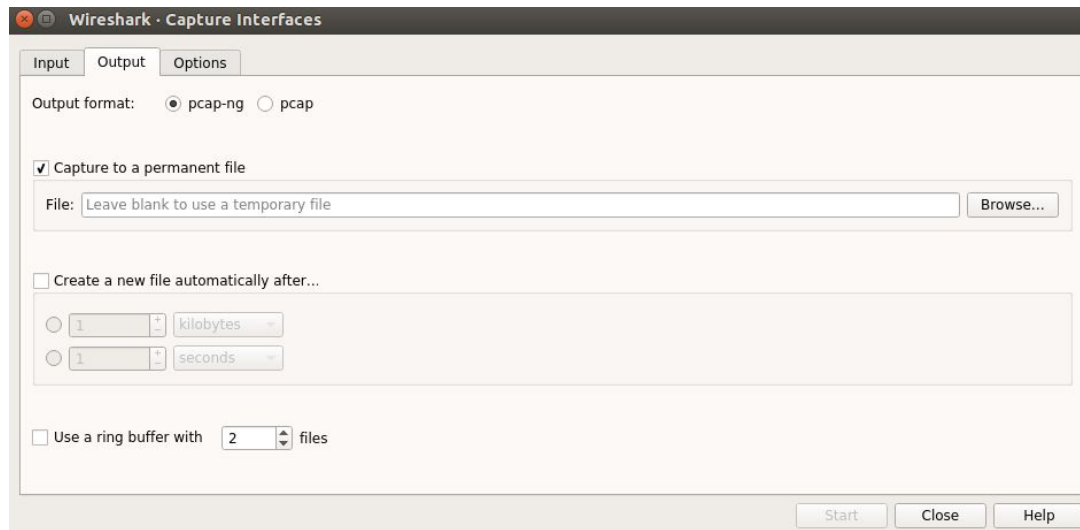
1. Abra um navegador web (fechar todas as demais páginas)
2. Inicie o Wireshark
3. No menu de captura, escolha “opções”
4. Selecione a sua interface local e marque para iniciar (*start*) a captura
5. Uma janela com diversos pacotes capturados irá aparecer
6. Marque o botão stop  para finalizar a captura, **mas não ainda!**
7. Vamos gerar um tráfego específico
8. Acesse a seguinte URL:  
<http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>
9. Pare a captura no Wireshark
10. Observe a lista extensa de pacotes
11. Escreva “http” sem as aspas para filtrar

## Primeira captura [2/2]

1. Encontre a mensagem HTTP GET que foi enviada do seu computador para o servidor HTTP `gaia.cs.umass.edu` (Procure por uma mensagem de HTTP GET na lista de pacotes capturados). Quando você selecionar, irá observar que os cabeçalhos do frame Ethernet, do datagrama IP, do segmento TCP e a mensagem HTTP. Ao clicar em + e - você pode ver os detalhes de cada um desses frames.

# Menu Output

- Você pode configurar a captura para ser salva em um arquivo permanente
  - No futuro você pode até importar capturas...



# Menu de Estatísticas

Navegue por este menu, faça uma análise das opções

# Exercício

Realizar para entregar no moodle um PDF de relatório.

1. Liste três diferentes protocolos que aparecem na coluna de protocolos quando não há filtros selecionados
2. Qual a diferença de tempo entre enviar um HTTP GET e receber um HTTP OK de resposta?
  - a. Utilize o comando ping do windows para ver a diferença. Como você pode explicar tal diferença (use o material de apoio no moodle para responder)
3. Qual é o endereço de IP do site gaia.cs.umass.edu? Qual o endereço IP de seu computador
4. Qual é o MAC do endereço origem e qual o endereço MAC do destino
  - a. Faça um *arp -a* no windows (cmd), quem é o MAC destino na rede local?
5. Cole um print das duas mensagens HTTP (GET e OK) da questão 2 acima.
6. Inicie uma nova captura, enquanto isso, assista ao vídeo no youtube: [https://youtu.be/ZRu47z\\_3ofs](https://youtu.be/ZRu47z_3ofs)
7. Ao final do vídeo finalize a captura
8. Mostre um gráfico da quantidade de pacotes transmitidos por segundo
9. Qual é o tamanho de pacotes mais frequente na captura que você realizou?