Centro Universitário 7 de Setembro
Sistemas de Informação
Redes de Computador I
1ª laboratório
Prof. Manoel Ribeiro

O Wireshark (anteriormente conhecido como Ethereal) é um programa que analisa o tráfego de rede, e o organiza por protocolos.

As funcionalidades do Wireshark são parecidas com o tcpdump mas com uma interface GUI, com mais informação e com a possibilidade da utilização de filtros.

Através dessa aplicação é possível controlar o tráfego de uma rede e monitora a entrada e saída de dados do computador, em diferentes protocolos, ou da rede à qual o computador está ligado.

Também é possível controlar o tráfego de um determinado dispositivo de rede numa máquina que pode ter um ou mais desses dispositivos.

Se você estiver numa rede local, com micros ligados através de um hub ou switch, outro usuário pode usar o Wireshark para capturar todas as suas transmissões.

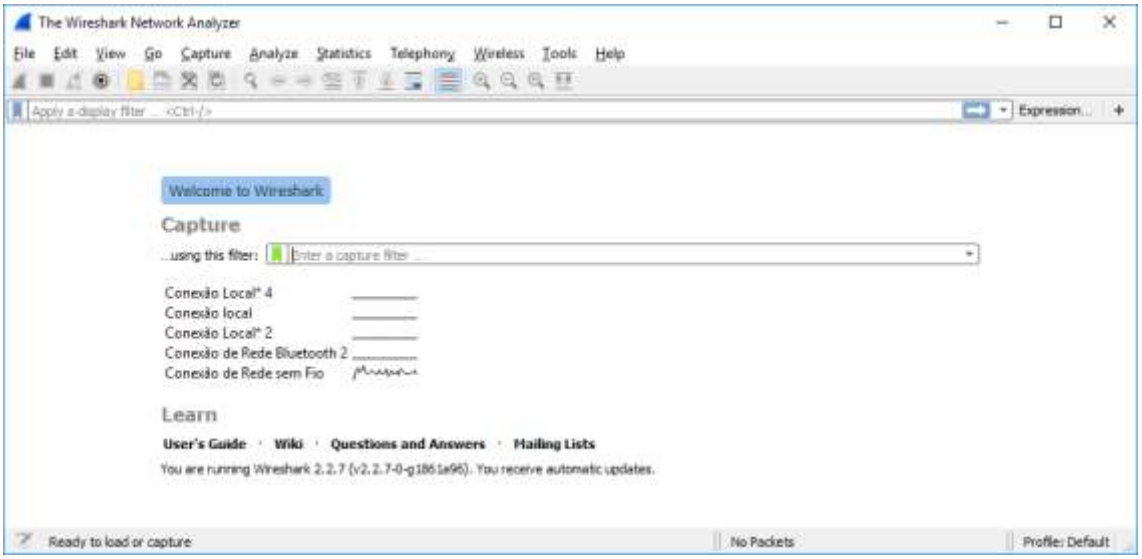
https://www.wireshark.org/download.html

Windows PortableApps® (32-bit)

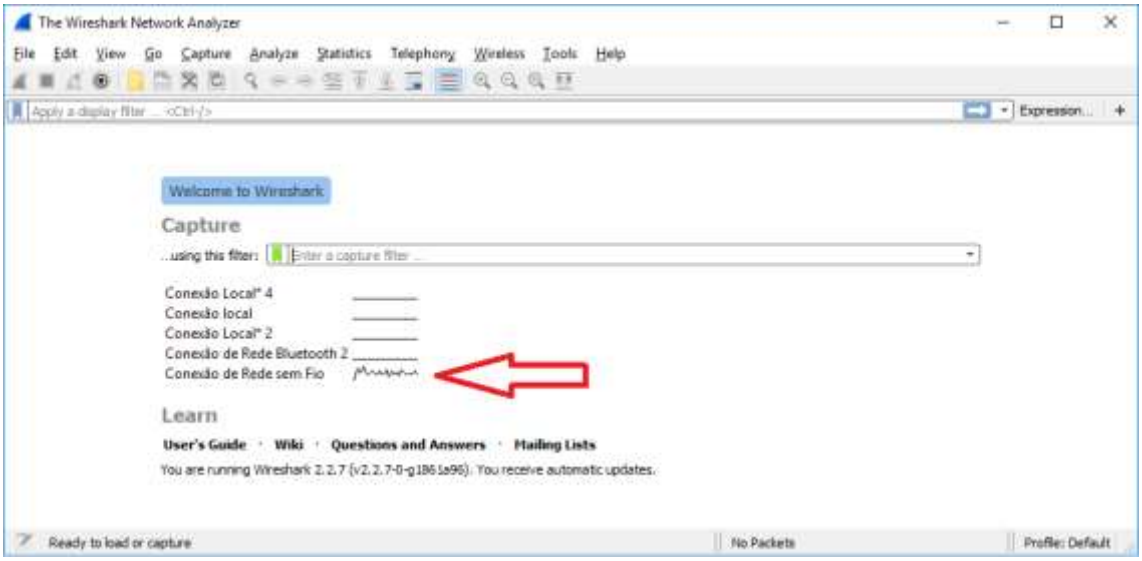
Centro Universitário 7 de Setembro
Sistemas de Informação
Redes de Computador I
1ª laboratório
Prof. Manoel Ribeiro

Prática

1. Entrar no Wireshark

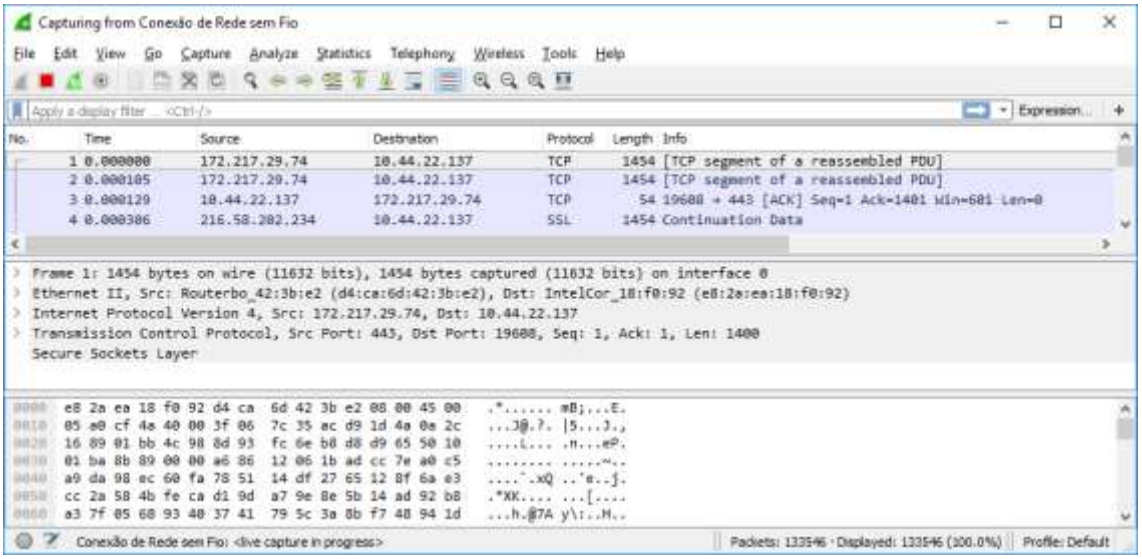


2. Identificar a conexão de rede ativa

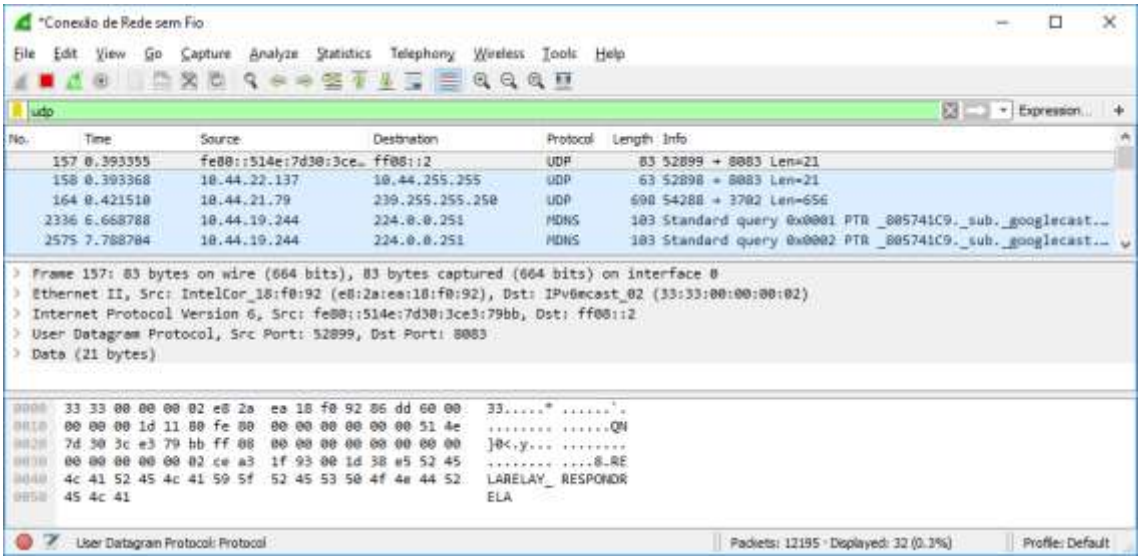


3. Selecionar a conexão de rede

Centro Universitário 7 de Setembro
Sistemas de Informação
Redes de Computador I
1ª laboratório
Prof. Manoel Ribeiro



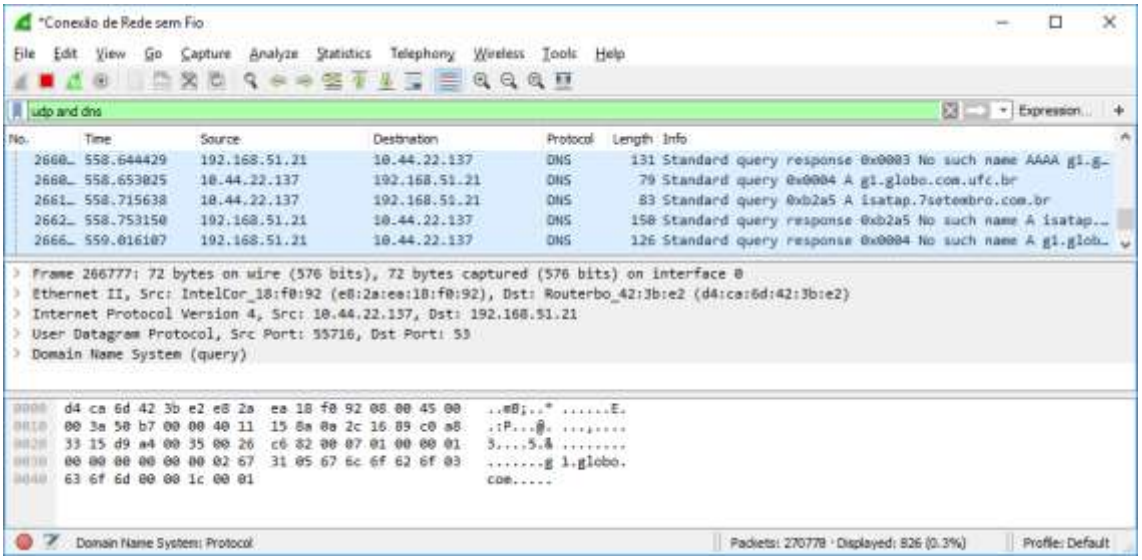
4. Aplicar filtro de UDP



5. Observar os protocolos de aplicação sobre o UDP
    - DNS - Domain Name System
    - MDNS - Multicast DNS
    - NBNS - NetBIOS Name Service
    - LLMNR - Link Local Multicast Name Resolution
    - SNMP - Simple Network Management Protocol
    - DHCP - Dynamic Host Configuration Protocol
    - DHCPv6 - Dynamic Host Configuration Protocol for IPv6

- SSDP - Simple Service Discovery Protocol

6. Adicionar filtro de DNS



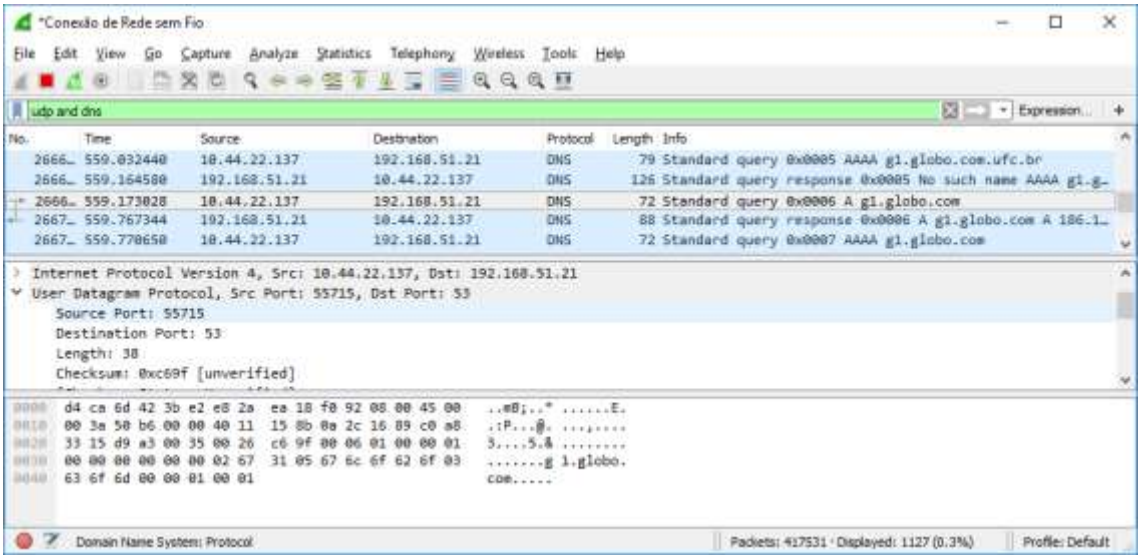
7. Forçar uma consulta DNS
   - nslookup g1.globo.com
8. Identificar os dois registros da consulta

   266699 559.173028 10.44.22.137 192.168.51.21
   DNS 72 **Standard query** 0x0006 A g1.globo.com

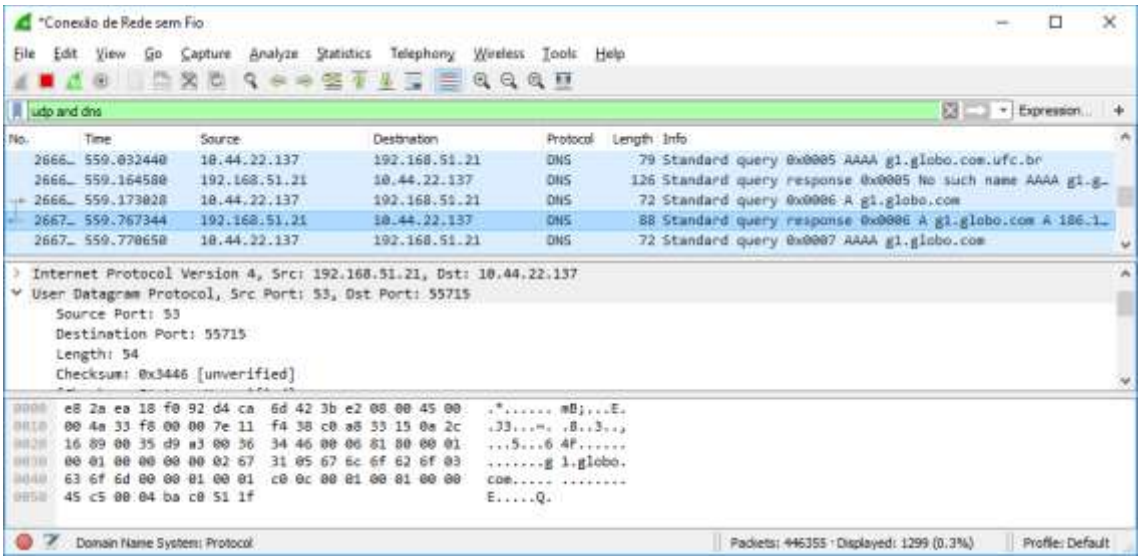
   266776 559.767344 192.168.51.21 10.44.22.137
   DNS 88 **Standard query response** 0x0006 A g1.globo.com A 186.192.81.31

9. Abrir o cabeçalho do pacote UDP da query na janela do meio

Centro Universitário 7 de Setembro
Sistemas de Informação
Redes de Computador I
1ª laboratório
Prof. Manoel Ribeiro



10. Observar o socket (portas)
11. Abrir o cabeçalho do pacote UDP da resposta



12. Observar o socket
13. Qual o socket na query?
14. Qual o socket na resposta?
15. Qual a conclusão?
16. Faça uma pesquisa sobre o risco de habilitar o protocolo SSDP.