Fatec São Caetano do Sul

Segurança em Sistemas Operacionais e Redes de Computadores II

Análise do conteúdo do tráfego – *Sniffer*

Análise do conteúdo do tráfego – *Sniffer*

Sniffing e *sniffers*

- Objetivo:

  Capturar tráfego de rede local para análise;
- A quem se destina:

  É útil tanto para atacantes como para administradores de rede.

Análise do conteúdo do tráfego – *Sniffer*

Sniffing e sniffers

- O atacante pode ler dados que passam por uma determinada máquina em tempo real ou guardar esses dados para futuro acesso;
- O administrador usa para detectar e resolver problemas.

Fatec São Caetano do Sul

Análise do conteúdo do tráfego – *Sniffer*

Tipos de dados capturados

- Qualquer coisa que é enviada pela rede e que não esteja encriptada:
  - nomes de usuários e senhas para sessões de telnet;
  - consultas e respostas a servidores de nomes (DNS);
  - mensagens de correio eletrônico;
  - senhas de FTP;
  - arquivos acessados através de NFS ou compartilhamentos do Windows;
  - etc..

Análise do conteúdo do tráfego – *Sniffer*

Modo promíscuo

- É o modo no qual a interface de rede captura todo o tráfego independentemente do endereço MAC de destino e pode ser utilizado em capturas de sniffing;
- Quando a interface de rede captura apenas o tráfego destinado a ela está no modo normal não-promíscuo.

Fatec São Caetano do Sul

Análise do conteúdo do tráfego – *Sniffer*

Acesso

- Para utilizar um sniffer é preciso ter uma conta de acesso à máquina onde está ou pode ser instalado o *sniffer*. Assim, empregados, fornecedores ou contratados podem se tornar atacantes se eles tem acesso a essas máquinas;
- Outras formas de acesso é através de exploração de vulnerabilidades através de ataques a aplicações e ao sistema operacional como por exemplo o ataque de "*buffer overflow*".

Fatec São Caetano do Sul

Análise do conteúdo do tráfego – *Sniffer*

Acesso

- Na maioria dos sistemas operacionais (incluindo o Windows e Linux), devido a limitações de acesso à leitura de pacotes diretamente de dispositivos de rede, o atacante necessita ter acesso de administrador.

Fatec São Caetano do Sul

Análise do conteúdo do tráfego – *Sniffer*

Sniffing através de hubs: sniffing passivo

- Em redes ligadas por hubs todas as interfaces recebem os dados destinados a todas elas "pegando" apenas os dados que lhes correspondem (todas as interfaces pertencem ao mesmo domínio de colisão);
- Se o atacante tiver uma interface nesse tipo de rede basta esperar passivamente pelos dados;
- Ferramentas: Snort (que evoluiu para um IDS), Sniffit e Wireshark

Fatec São Caetano do Sul

Análise do conteúdo do tráfego – *Sniffer*

Sniffing ativo: *sniffing* através de *switches*

- Nos *switches* cada porta é um domínio de colisão separado ou seja o tráfego é enviado apenas para o destinatário (porta cuja interface tem o endereço de MAC de destino);
- Para superar essa dificuldade são utilizadas ferramentas que ativamente injetam tráfego na LAN;
- Ferramentas: Dsniff e Ettercap.

Fatec São Caetano do Sul

Análise do conteúdo do tráfego – *Sniffer*

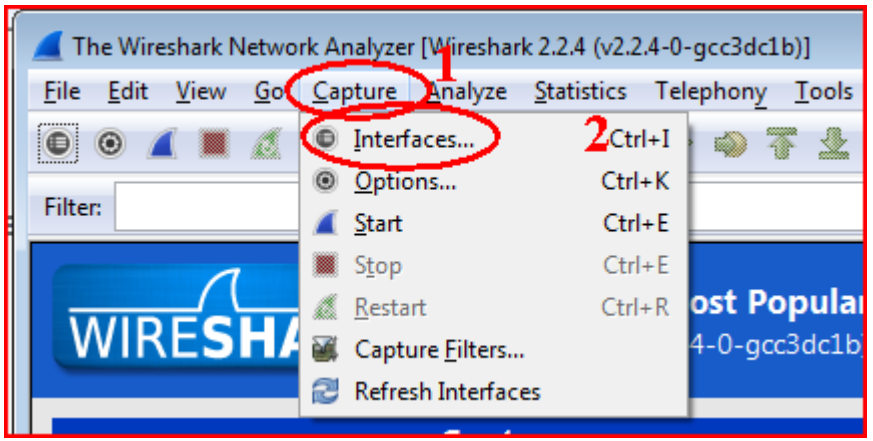
Wireshark (evoluiu do Ethereal)

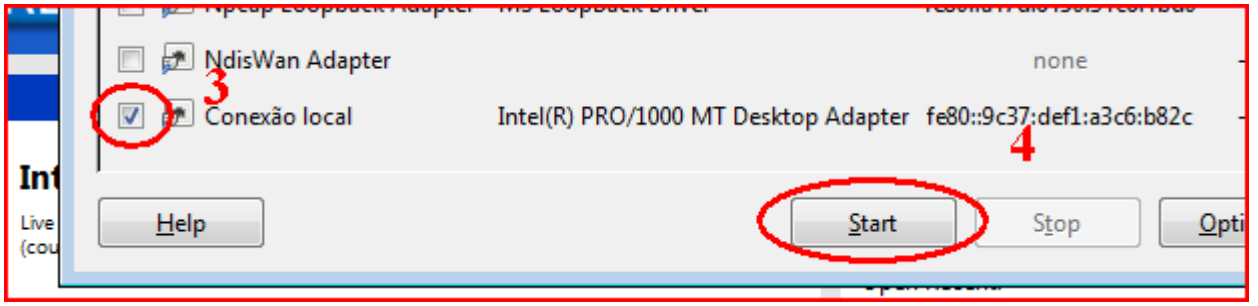
- A ferramenta de análise e rastreamento de pacotes mais popular;
- Software livre (GNU GPL);
- Muitas opções.

Análise do conteúdo do tráfego – *Sniffer*

Wireshark

- Escolha da interface e inicio da captura



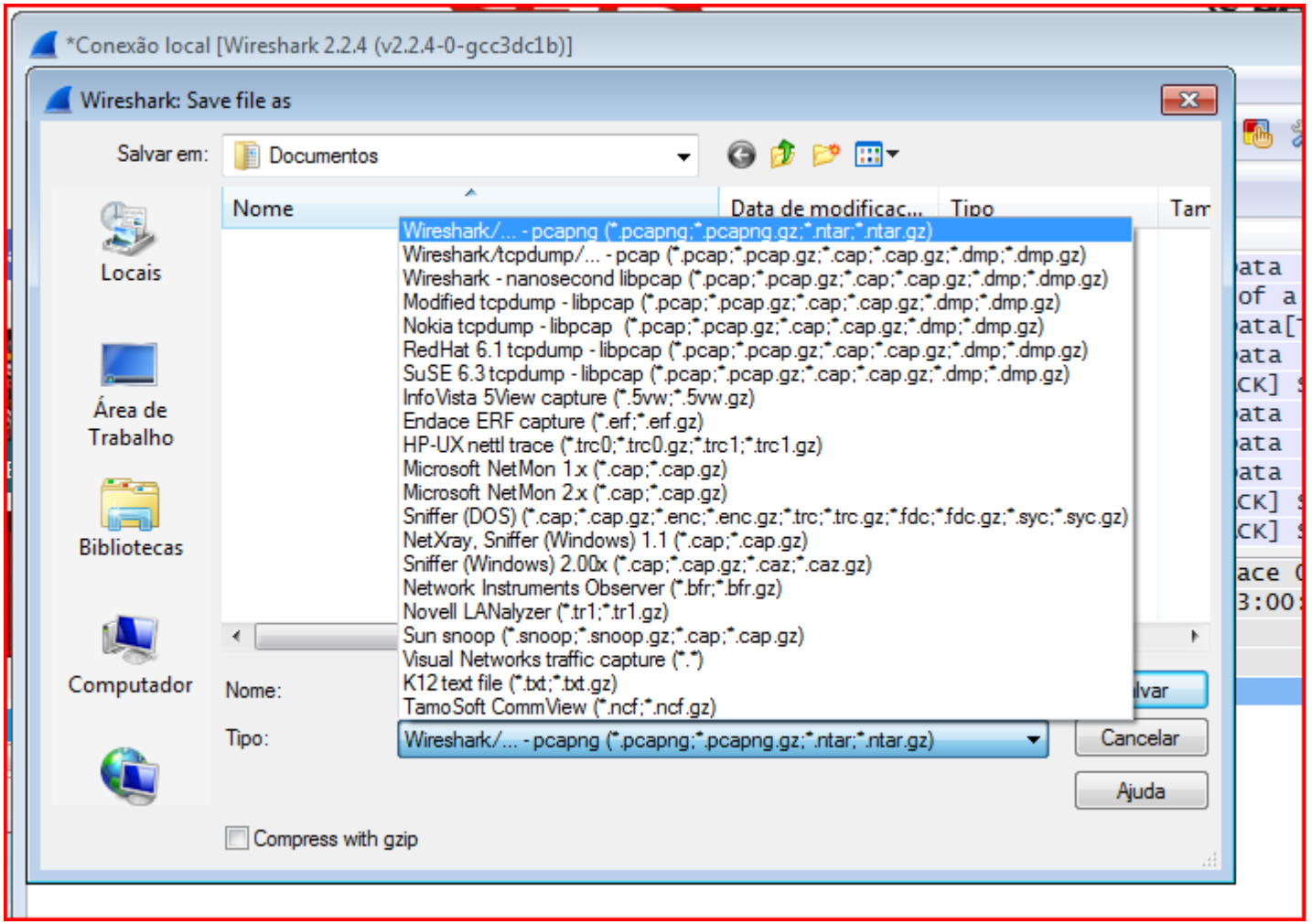


Fatec São Caetano do Sul

Análise do conteúdo do tráfego – *Sniffer*

Wireshark

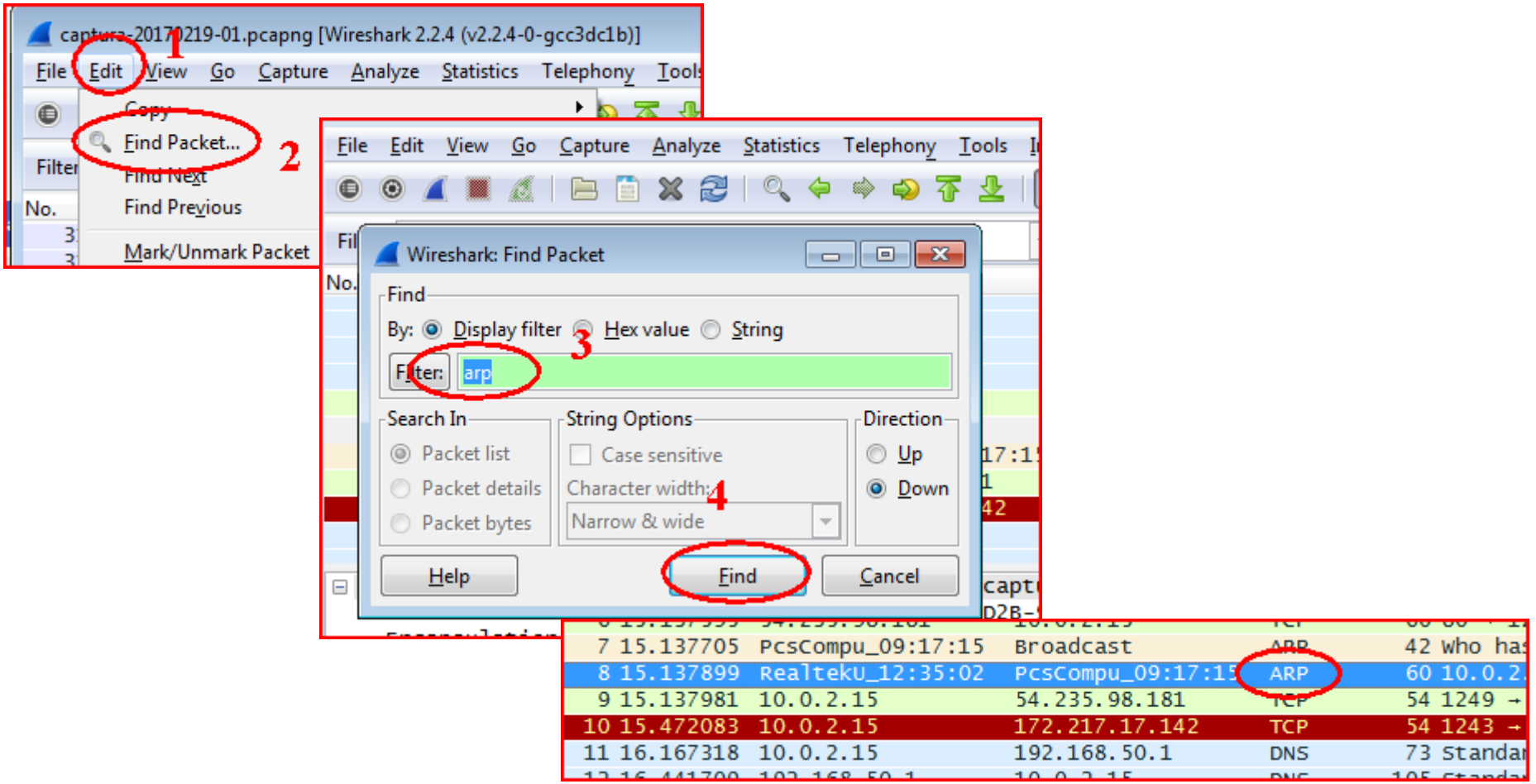
- É possível guardar e abrir arquivos de capturas em uma grande variedade de formatos.



Análise do conteúdo do tráfego – *Sniffer*

Wireshark

- Encontrar pacotes

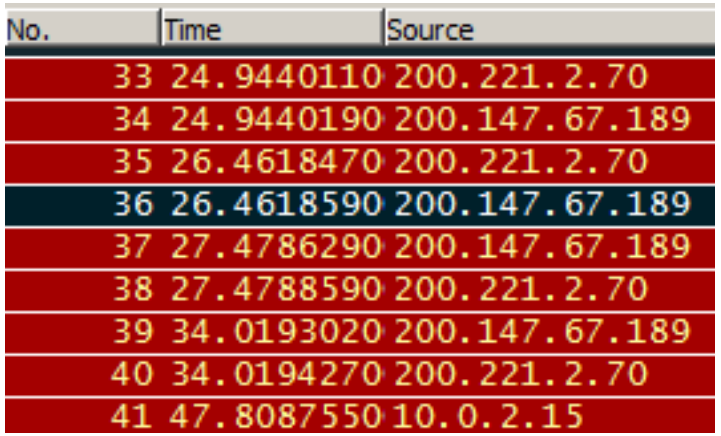


Análise do conteúdo do tráfego – *Sniffer*

Wireshark

- Marcar e desmarcar pacotes

Edit → Mark/Unmark Packet



No.	Time	Source
33	24.9440110	200.221.2.70
34	24.9440190	200.147.67.189
35	26.4618470	200.221.2.70
36	26.4618590	200.147.67.189
37	27.4786290	200.147.67.189
38	27.4788590	200.221.2.70
39	34.0193020	200.147.67.189
40	34.0194270	200.221.2.70
41	47.8087550	10.0.2.15

No.	Time	Source	Des
33	24.9440110	200.221.2.70	10
34	24.9440190	200.147.67.189	10
35	26.4618470	200.221.2.70	10
36	26.4618590	200.147.67.189	10
37	27.4786290	200.147.67.189	10
38	27.4788590	200.221.2.70	10
39	34.0193020	200.147.67.189	10
40	34.0194270	200.221.2.70	10
41	47.8087550	10.0.2.15	18

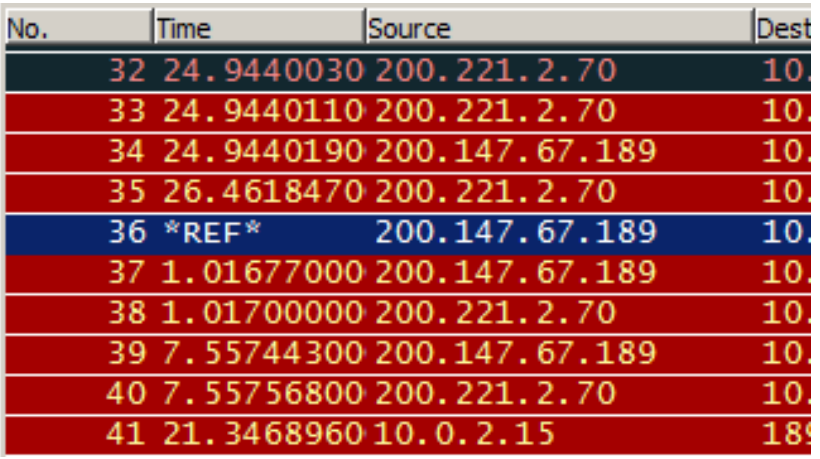
Análise do conteúdo do tráfego – *Sniffer*

Wireshark

- Estabelecer referência de tempo

Edit → Set/Unset Time Reference

No.	Time	Source	Des
33	24.9440110	200.221.2.70	10
34	24.9440190	200.147.67.189	10
35	26.4618470	200.221.2.70	10
36	26.4618590	200.147.67.189	10
37	27.4786290	200.147.67.189	10
38	27.4788590	200.221.2.70	10
39	34.0193020	200.147.67.189	10
40	34.0194270	200.221.2.70	10
41	47.8087550	10.0.2.15	18



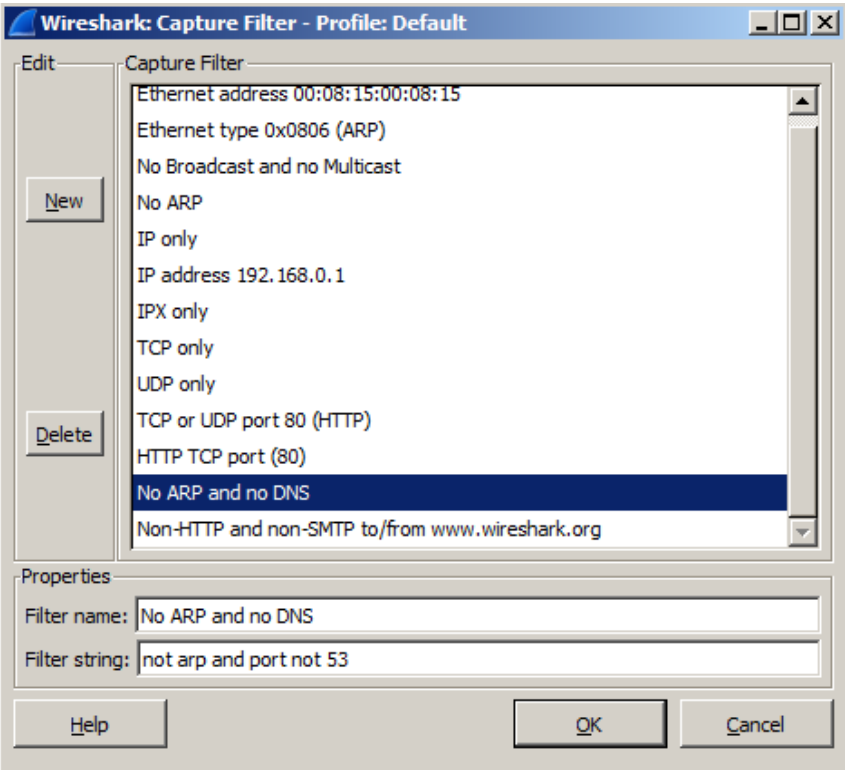
No.	Time	Source	Dest
32	24.9440030	200.221.2.70	10.
33	24.9440110	200.221.2.70	10.
34	24.9440190	200.147.67.189	10.
35	26.4618470	200.221.2.70	10.
36	*REF*	200.147.67.189	10.
37	1.01677000	200.147.67.189	10.
38	1.01700000	200.221.2.70	10.
39	7.55744300	200.147.67.189	10.
40	7.55756800	200.221.2.70	10.
41	21.3468960	10.0.2.15	18

Análise do conteúdo do tráfego – *Sniffer*

Wireshark

- Estabelecer filtros de captura ou usar os preestabelecidos

Capture → Capture Filters...

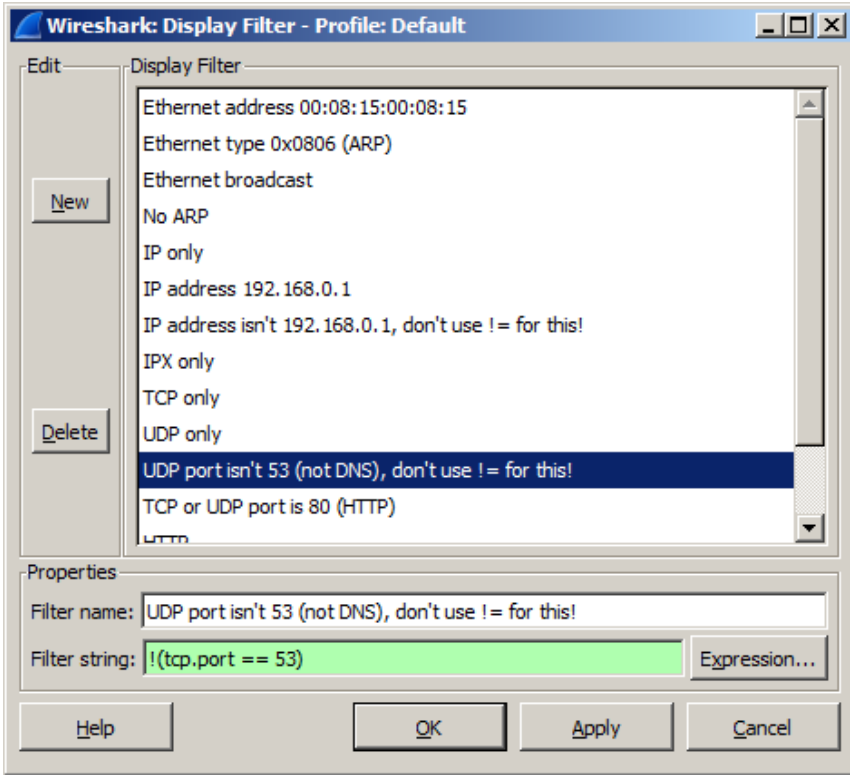


Análise do conteúdo do tráfego – *Sniffer*

Wireshark

- Estabelecer filtros de apresentação ou usar os preestabelecidos

Analyze → Display Filters...



Fatec São Caetano do Sul

Análise do conteúdo do tráfego – *Sniffer*

Fontes:

- wireshark.org;
- SKODIS E., LISTON T. **Counter Hack Reloaded**, Second Edition: A Step-by-Step Guide to Computer Attacks and Effective Defenses