ESCOLA SUPERIOR DE TECNOLOGIA DE ABRANTES
INSTITUTO POLITÉCNICO DE TOMAR

Redes de Comunicação / Redes de Computadores e Administração de Sistemas

Apoio 2
Utilização do *Packet Sniffer* Wireshark

Disciplina do 1º ano, 2º Semestre, TeSP Informática

Disciplina do 2º ano, 2º Semestre, Lic. em Informática e Tecnologias Multimédia

Docente Responsável

Valter Bouça
vbouca@ipt.pt

2017-18

Introdução ao Wireshark

1. Analisador de pacotes

Um analisador de pacotes (*packet sniffer*) é uma aplicação que captura os pacotes que flúem numa rede, permitindo a sua análise. Contrariamente às restantes aplicações, que apenas analisam os pacotes a si destinados, um *sniffer* pode actuar em modo promíscuo, analisando todo o tráfego que passa no ponto de rede onde está ligado. A sua correcta utilização permite identificar problemas na rede que de outra forma seriam de difícil detecção.

2. Cuidados na utilização de um *sniffer*

Tal como quase todas as ferramentas, um *sniffer* pode também ser usado para fins menos próprios. O facto de puder capturar tráfego que não lhe é destinado faz com que possa por em causa a privacidade de quem utiliza a rede, se for utilizado de forma indevida. Além disso, alguns protocolos de comunicação usam métodos pouco seguros para envio de informação importante, como por exemplo a validação por palavra-chave num servidor de mail POP3 que é enviada sem protecção, podendo essa informação ser capturada e usada para fins indevidos.

O tráfego capturado pelo *sniffer* corresponde apenas ao tráfego que lhe chega da rede. Se estiver colocado num repetidor onde estão vários outros dispositivos, será capaz de aceder a muito tráfego, mas se estiver ligado a um switch será apenas capaz de ver alguns tipos de pacotes.

3. Instalação e configuração

Efectue o descarregar do Wireshark em http://www.wireshark.org. Para o seu correcto funcionamento, o Wireshark necessita ainda de uma biblioteca de funções, chamada WinPcap, comum a várias aplicações do tipo. As versões de distribuição mais recentes incluem esta biblioteca, que também pode ser obtida em http://netgroup-serv.polito.it/winpcap/ . Versões mais antigas do WinPcap podem não funcionar correctamente com o Windows XP SP2 e Windows 2003, pelo que será conveniente ter uma versão actualizada do mesmo instalada.

O Wireshark era inicialmente denominado Ethereal. Devido a uma disputa legal recente, os responsáveis do projecto tiveram de alterar essa designação.

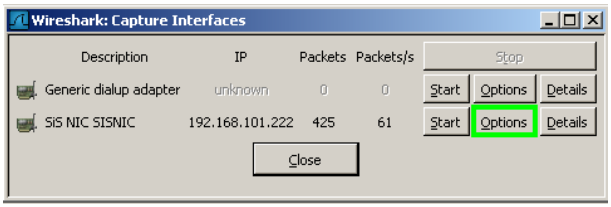
4. Utilização de filtros

Numa rede de elevado tráfego, o volume de informação em trânsito pode ser muito elevado, pelo que será conveniente no processo de captura definir quais os tipos de pacotes a obter. Para tal é definido um filtro de captura. O Wireshark tem inicialmente definidos alguns filtros mais utilizados, sendo o processo de criação de novos filtros bastante simples. Além do filtro de captura pode ainda utilizar um filtro de visualização que escolhe, dentro dos pacotes capturados, quais os que serão visualizados numa determinada altura. Pode mudar de filtros de visualização sem ter de fazer uma nova captura. Pode obter mais informação sobre filtros em http://wiki.ethereal.com/CaptureFilters ou no manual online em http://www.ethereal.com/docs/eug_html_chunked/ChCapCaptureFilterSection.html.

5. Iniciando uma captura

1. Seleccione o interface sobre o qual vai efectuar a captura.

2. Define as opções de captura para esse interface.

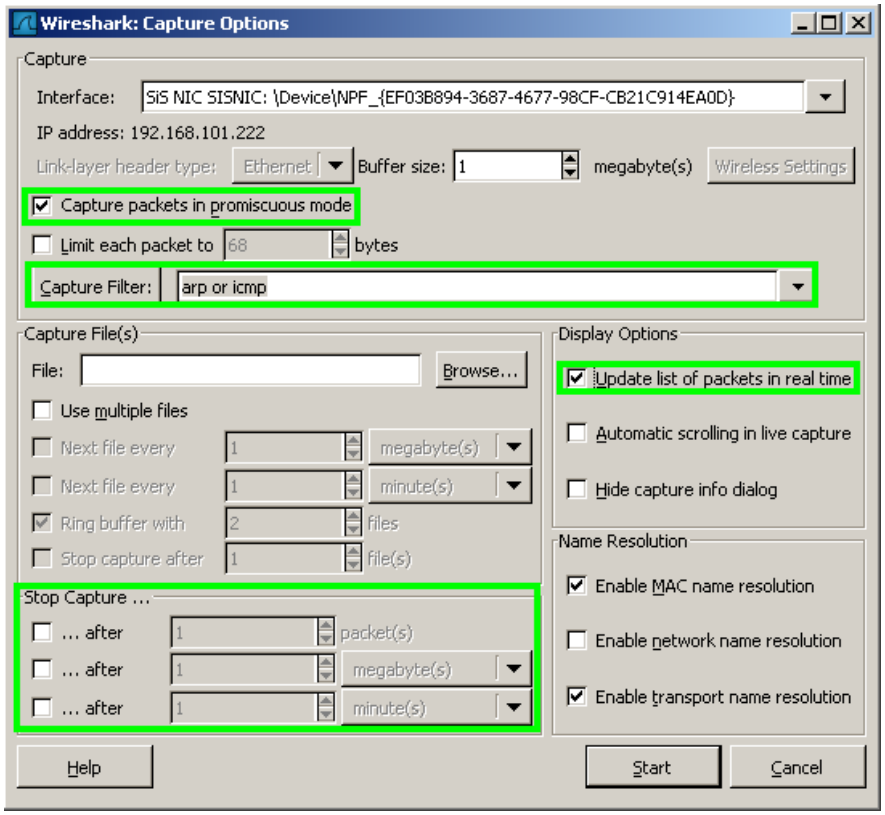


3. Se pretende capturar todo o tráfego na rede, e não apenas o destinado ao interface seleccionado, escolha a captura em modo promíscuo.

Defina o filtro de captura.

Escolha a opção "Update… in real time" para ir poder aceder aos pacotes à medida que vão sendo capturados e não apenas quando terminar a captura.

Pode configurar a captura para terminar automaticamente.

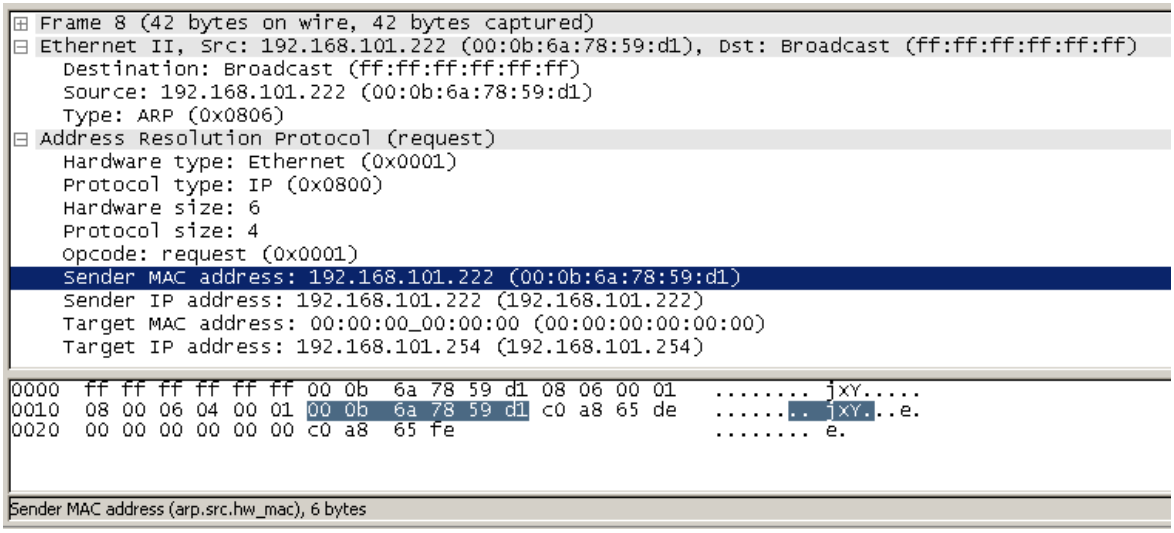


4. Durante o processo de captura são-lhe fornecidas estatísticas sobre os pacotes que foram capturados da rede (mesmo os que não estão a ser visualizados).

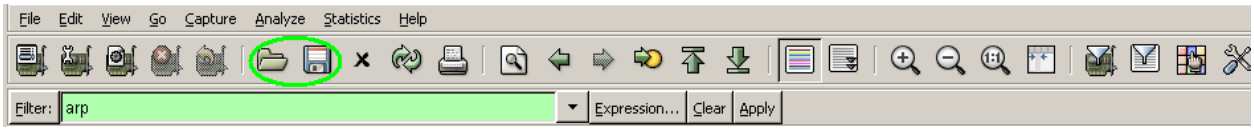
5. O Wireshark analisa os pacotes e coloca a informação mais importante de forma facilmente perceptível.

```
  7 11.442341   192.168.101.75    Broadcast         ARP    Who has 192.168.101.28?  Tell 192.168.101.75
  8 16.815266   192.168.101.222   Broadcast         ARP    Who has 192.168.101.254?  Tell 192.168.101.22
  9 16.815403   192.168.101.254   192.168.101.222   ARP    192.168.101.254 is at 00:50:fc:a2:1e:1c
```

6. Caso pretenda obter mais informação sobre um determinado pacote, seleccione-o. Poderá visualizar o pacote em estado "bruto" ou ver a informação associada que a aplicação vai disponibilizando.



7. Pode armazenar as capturas para posterior análise.



8. Não se esqueça que pode definir filtros de visualização (e captura). O Wireshark disponibiliza alguns filtros pré-definidos, mas pode criar os seus.