Trabalho Nº 1 - Ethereal

1. Objectivos do Trabalho

- Tomar conhecimento com um analisador de pacotes
  - Ethereal
- Realizar capturas de pacotes e analisá-los
  - TCP / UDP
  - IP
  - Ethernet
  - HTTP / DNS …

2. Ambiente de trabalho

Linux ou Windows

Efectuar a verificação da disponibilidade e configuração do ambiente de trabalho e desenvolvimento a utilizar nos exercícios de práticos da cadeira.

Analisador de protocolos – Ethereal
Pretende-se efectuar a aprendizagem das principais funcionalidade e opções do analisador de pacotes - o Ethereal - que irá ser utilizado para análise dos protocolos.

Nota: Durante a execução deste exercício deverá efectuar a recolha / captura de elementos para ilustrar o relatório a apresentar ao professor. Para tal deverá utilizar um utilitário de Screen Capture, do tipo do KSnapshot

3. Realização do Trabalho

Para executar o programa Ethereal em Linux, deverá executar o seguinte comando numa consola:

sudo ethereal

Se tudo estiver bem configurado, o comando irá pedir a sua password de aluno, e depois irá executar-se normalmente.

Em Windows, se o programa estiver instalado, basta clickar no respectivo incone.

Será apresentada a interface gráfica representada na figura 1 (embora sem dados):

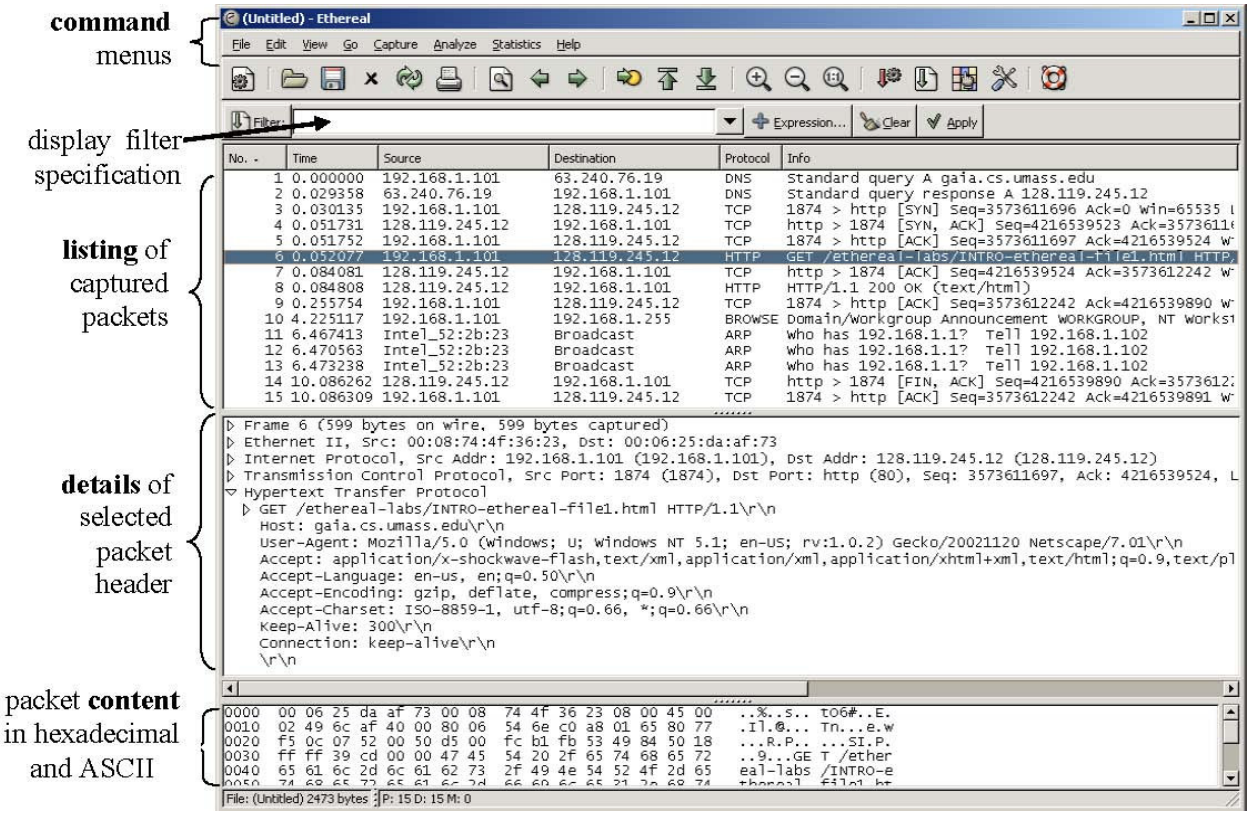

Figura 1: Interface Gráfica do Ethereal

3.1 Utilização do programa Ethereal

A melhor forma de aprender qualquer programa é utilizá-lo! Fazer o seguinte:

1. Iniciar o browser seleccionando a Homepage do Laboratório.

2. Iniciar o programa Ethereal. Será visualizada uma janela idêntica à da Figura 1 mas sem dados (ainda não foi iniciada a captura de pacotes).

3. Utilizando a opção apropriada do programa verifique quais os interfaces disponíveis.

4. Para iniciar a captura, seleccione o pull down menu - Capture e seleccione a opção Start. Visualizará a janela “Ethereal: Capture Options”, conforme mostrado na figura 2.

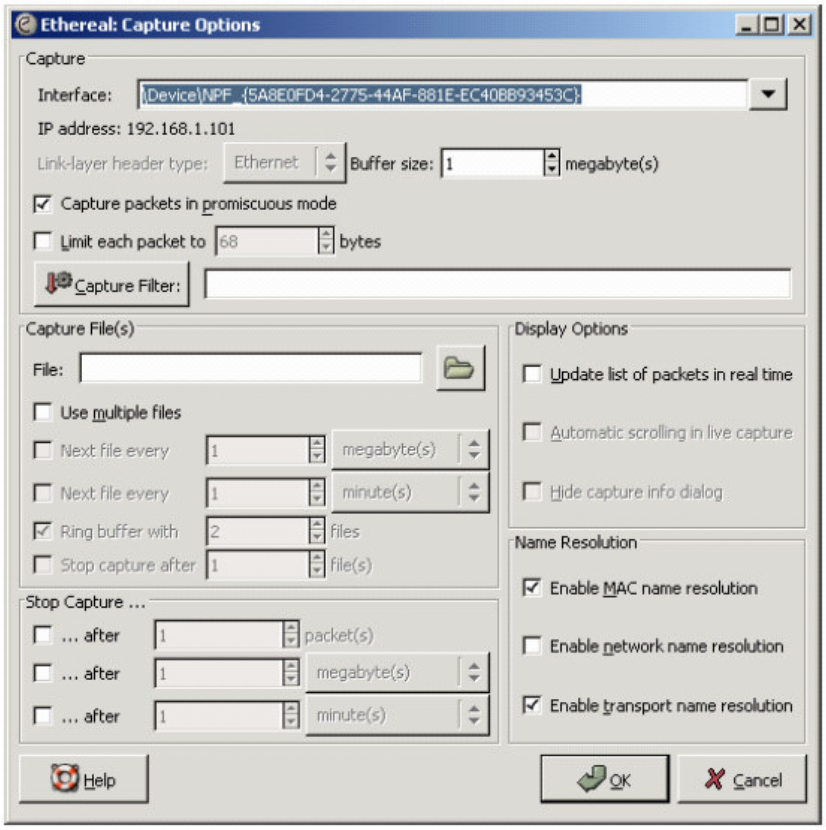

Figura 2: Opções de Captura do Ethereal

5. Todas as interfaces de rede (i.e., ligações físicas) que o computador tem serão mostradas no “pull down menu” no topo da janela “Capture Options”. No caso do computador ter mais que uma interface de rede activa (e.g., se existem ligações wireless e ligação fixa Ethernet), será necessário seleccionar a interface que será utilizada para enviar e receber pacotes (geralmente a ligação fixa). É preferível seleccionar as opções “Update list of Packets in Real Time” e “Automatic Scrolling in live Capture” para ter a noção dos pacotes que estão a ser capturados. A opção Hide Capture info Dialog permite esconder uma outra janela que aparece durante a captura onde é apresentado um resumo estatístico dos pacotes capturados.

6. Depois de seleccionada a interface de rede (ou utilizar a interface por defeito escolhida pelo Ethereal), premir OK. A captura de pacotes será iniciada – sendo todos os pacotes enviados e recebidos do e para o seu computador capturados pelo Ethereal.

7. Uma vez iniciada a captura de pacotes, uma janela de resumo de captura de pacotes irá aparecer conforme indicado na figura 3. Esta janela resume o número de pacotes dos vários tipos que são capturados, e (importante!) contém o botão Stop que permite parar a captura de pacotes. Não parar ainda!

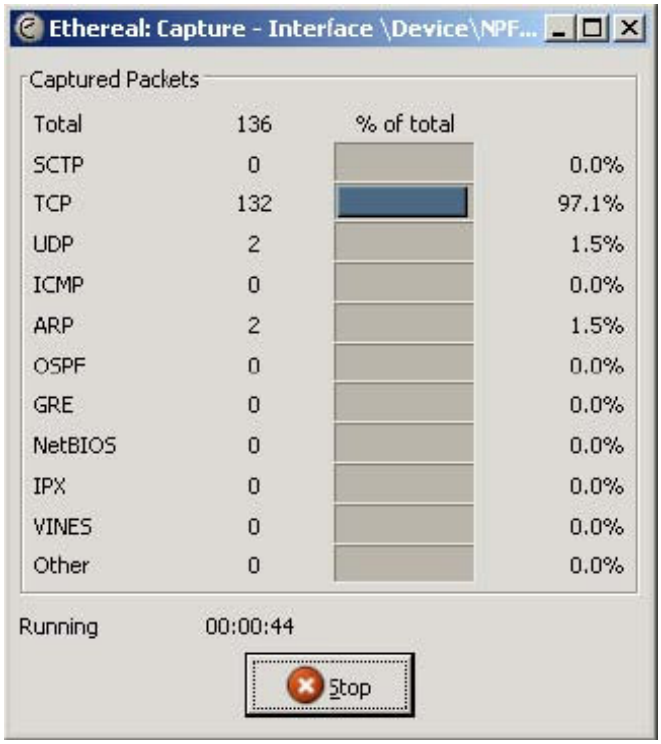

Figura 4: Janela de Resumo da Captura de Pacotes

8. Depois de iniciada a captura no Ethereal, aceda com o seu browser ao URL: http://srv1.inetlab.ulusofona.pt. Para visualizar esta página, o browser contacta o servidor Web do Laboratório e troca mensagens HTTP para fazer o download da página acedida. As frames Ethernet contendo essas mensagens serão capturadas pelo Ethereal.

   Se desejar, poderá aceder a outro site da sua preferência, só que nesse caso o número de pacotes e de mensagens poderá ser muito mais elevado.

9. Depois de visualizar as páginas indicadas no ponto anterior, pare a captura de pacotes Ethereal seleccionando a opção stop na janela de captura. A janela Ethereal será agora semelhante à da Figura 1. Teremos agora os pacotes reais que contém todas as mensagens dos protocolos trocadas entre o seu computador e as outras entidades de rede. As mensagens HTTP trocadas com os servidores Web srv1.inetlab.ulusofona.pt ou outro que tenha seleccionado, serão apresentadas na lista de pacotes capturados. Existirão inúmeros pacotes de outro tipo também mostrados (verificar os vários e diferentes tipos de protocolos mostrados na coluna Protocol na Figura 1). Poderá filtrar os protocolos que lhe interessam utilizando o menu Filter.

10. Guardar em ficheiro local os pacotes capturados, através da opção File > Save As. Convém guardar as capturas em ficheiros organizados em pastas por trabalho.

11. Filtragem por tipo de protocolo: digitar “http” (sem as aspas, e em minúsculas – todos os nomes de protocolos estão em minúsculas no Ethereal) na janela de “Filter” do Ethereal. Depois seleccione “Apply”. Como resultado, apenas as mensagens HTTP serão visualizadas.

12. Seleccionar a primeira mensagem http mostrada na janela “packet-listing”. Deverá

ser a mensagem HTTP GET a primeira que foi enviada do seu computador para o servidor Web srv1.inetlab.ulusofona.pt. Quando seleccionar a mensagem HTTP GET, a frame Ethernet, o datagrama IP, o segmento TCP, e o cabeçalho de informação da mensagem HTTP serão mostrados na janela de visualização de cabeçalho de pacotes. Clicke nas setas para a direita/esquerda e baixo/cima e verifique o resultado, minimizando a quantidade de Frames, Ethernet, Internet Protocol, e Transmission Control Protocol mostradas. Maximize a quantidade de informação mostrada do protocolo HTTP. A janela do programa Ethereal será aproximadamente semelhante ao exemplo da figura 4.

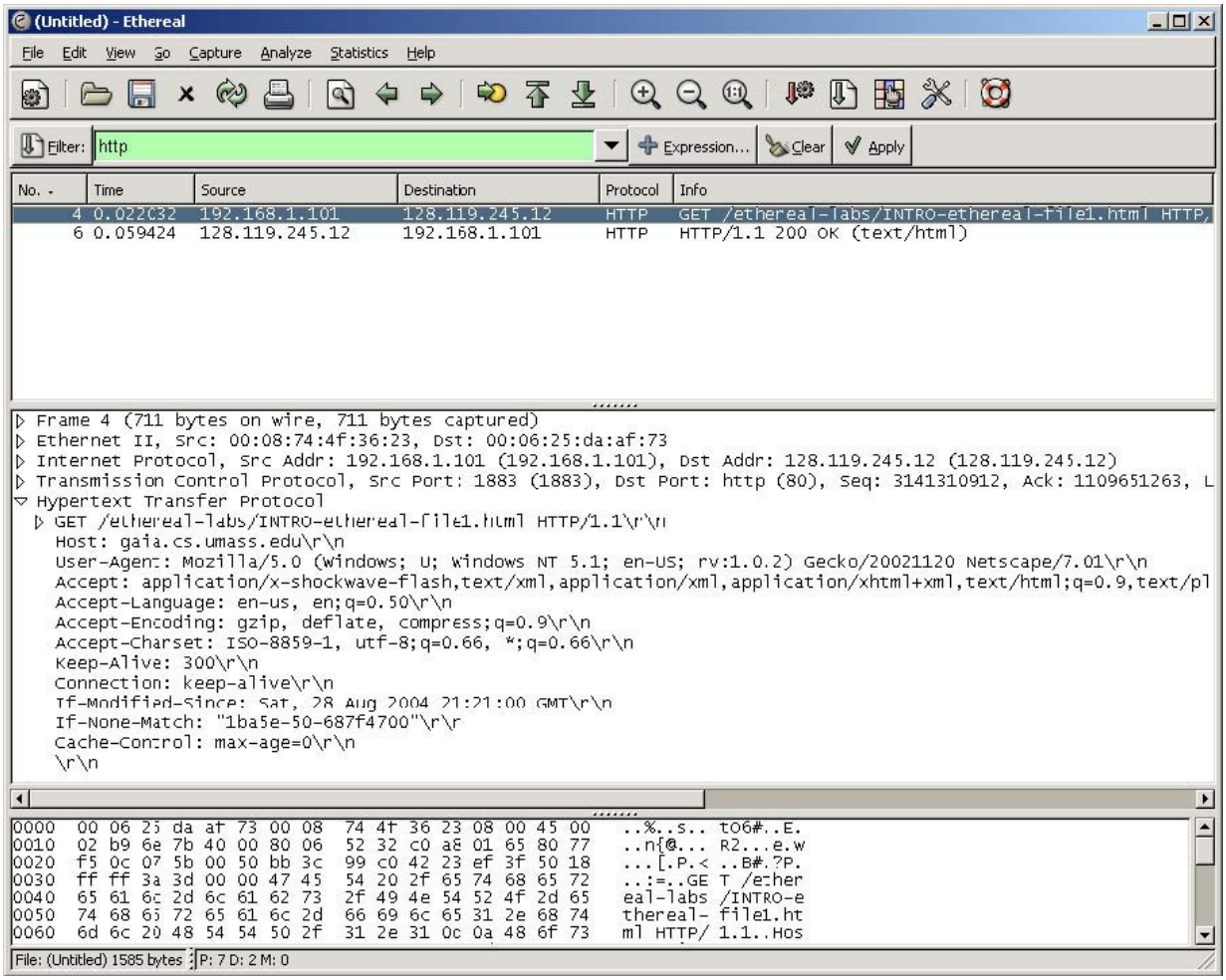

Figura 4: Filtragem por HTTP.

13. Saia do programa Ethereal, não sem esquecer de guardar o ficheiro das capturas que efectuou.

4. Análise Final

O objectivo essencial deste primeiro exercício de laboratório foi o de realizar uma primeira introdução ao programa Ethereal, assim como ficar com uma primeira noção do que são mensagens e protocolos.

As seguintes questões demonstrarão que conseguiu activar o Ethereal, e que foram exploradas algumas das suas capacidades.

No relatório a apresentar, responda às seguintes perguntas, baseando-se nos resultados e imagens que armazenou no decorrer da sua interacção com o Ethereal:

1. Liste os diferentes protocolos que aparecem na coluna "protocol" na lista de pacotes sem qualquer filtro após o ponto 8 acima.

2. Quanto tempo demorou desde que a mensagem HTTP GET foi enviada até que a resposta HTTP OK foi recebida? (Por defeito, o valor do tempo na coluna "Time" é a quantidade de tempo em segundos, desde que o trace do Ethereal começou.

3. Para se visualizar o campo "Time" no formato "time-of-day", seleccionar o menu *View* no menu "pull down", e depois seleccionar "Time *Display Format"*, e depois "*Time-of-day"*.

4. Quais são os endereços IP do servidor srv1.inetlab.ulusofona.pt ou de outro site a que tenha acedido? Qual é o endereço IP do seu computador?

   Capture (utilizando o utilitário KSnapShot) o detalhe das duas mensagens HTTP mostradas no ponto 10 acima e insira as respectivas imagens no seu relatório.

5. Entrega do Trabalho

O prazo para a entrega deste trabalho é de uma semana a contar da aula em que o enunciado foi apresentado. Não serão aceites trabalhos fora do prazo.

A entrega deverá ser feita por e-mail num ficheiro zip (ou rar) contendo um relatório em PDF e as imagens capturadas ou listagens dos programas realizados, obedecendo OBRIGATORIAMENTE ao seguinte formato:

`a123456-trabalho-N.zip`

6. Referências

"Ethereal: A Network Protocol Analyzer" http://www.ethereal.com

"Enciclopédia of Networking and Telecommunications" http://www.linktionary.com/linktionary.html