Universidade Federal do Ceará (UFC) - Campus Quixadá
Disciplina: Redes de Computadores Período 2011:1
Profa. Atslands Rego da Rocha (atslands@ufc.br)
Data: 01/03/2011

01 AULA PRÁTICA – INTRODUÇÃO SNIFFER DE PACOTES (WIRESHARK)

(Baseada nas Práticas do livro de James Kurose – 4Edição)

Um sniffer de pacotes (sniffer packet) é uma ferramenta básica para observação das mensagens trocadas entre as entidades da rede. Como o nome sugere, um sniffer de pacotes captura ("sniffs" = "fareja") mensagens que estão sendo enviadas/recebidas pelo seu computador. Ele também irá tipicamente armazenar e/ou mostrar os conteúdos de vários campos de protocolo nessas mensagens capturadas. Um sniffer de pacotes é uma ferramenta passiva, ou seja, ele observa as mensagens sendo enviadas/recebidas pelas aplicações e protocolos em execução no seu computador, mas ele nunca envia pacotes por si próprio. Da mesma forma, os pacotes recebidos não são explicitamente endereçados ao sniffer de pacotes. Ao invés disso, ele recebe uma *cópia* dos pacotes que estão sendo enviados/recebidos de/para as aplicações e protocolos em execução da sua máquina. Na verdade, é a biblioteca de capturas de pacotes (packet capture library) quem recebe uma cópia de todo quadro da camada de enlace que é enviado/recebido de/para seu computador. O segundo componente de um sniffer de pacotes é o analisador de pacotes (packet analyzer), que mostra os conteúdos de todos os campos de uma mensagem. Ele também "compreende" a estrutura de todas as mensagens trocadas entre os protocolos. Observe a Figura 1 que ilustra a estrutura de um sniffer de pacotes com todos os seus elementos.

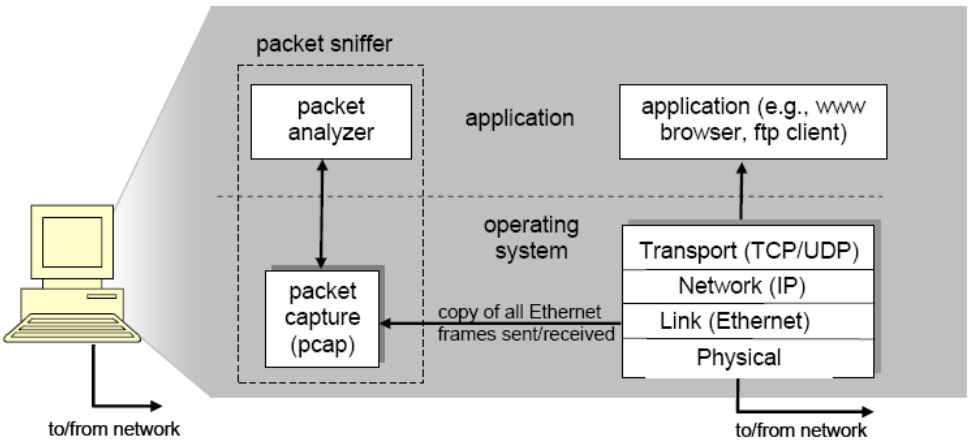

Figura 1. Estrutura de um sniffer de pacotes

De acordo com as práticas explicadas no livro do James Kurose versão 4 (e diferentemente da versão 3), utilizaremos a ferramenta gratuita chamada Wireshark que pode ser encontrada em http://www.wireshark.org/ para Windows/Linus/OS X. Se desejar um aprofundamento no tema, aproveite a documentação disponibilizada no site da ferramenta.

Executando Wireshark pela primeira vez

Vamos aprender a usar a ferramenta. Para isso, siga os passos abaixo:

1. Inicie seu navegador (browser) favorito que mostrará sua página inicial pré-selecionada.
2. Execute o Wireshark. Quando a execução do Wireshark iniciar, uma interface gráfica como a ilustrada na Figura 2 aparecerá. Você poderá escolher documentação, amostras de traces, entre outras coisas. Neste momento, escolha a interface de rede que deseja monitorar na lista apresentada na ferramenta.

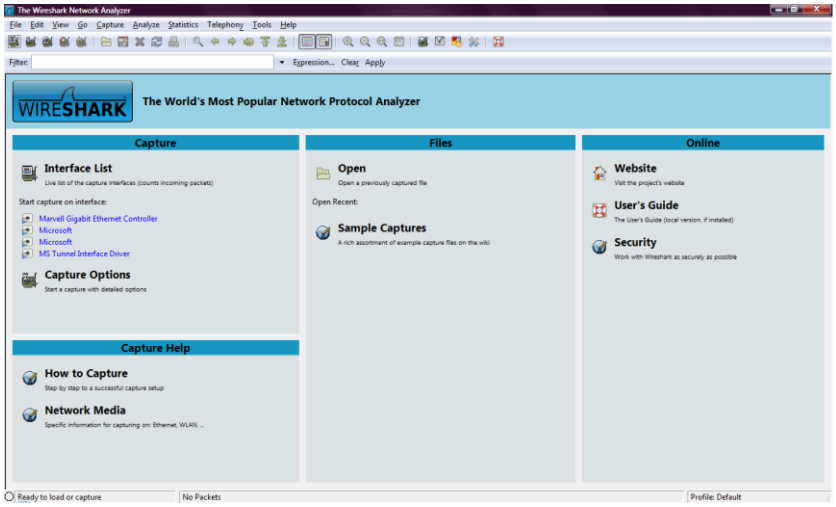

Figura 2. Menu Inicial Wireshark

Após a seleção da interface de rede, uma interface gráfica como a ilustrada na Figura 3 aparecerá.

Nota: Se você já estiver na interface gráfica mostrada na Figura 3, para iniciar uma nova captura, selecione a opção "Capture" no menu e selecione "Start".

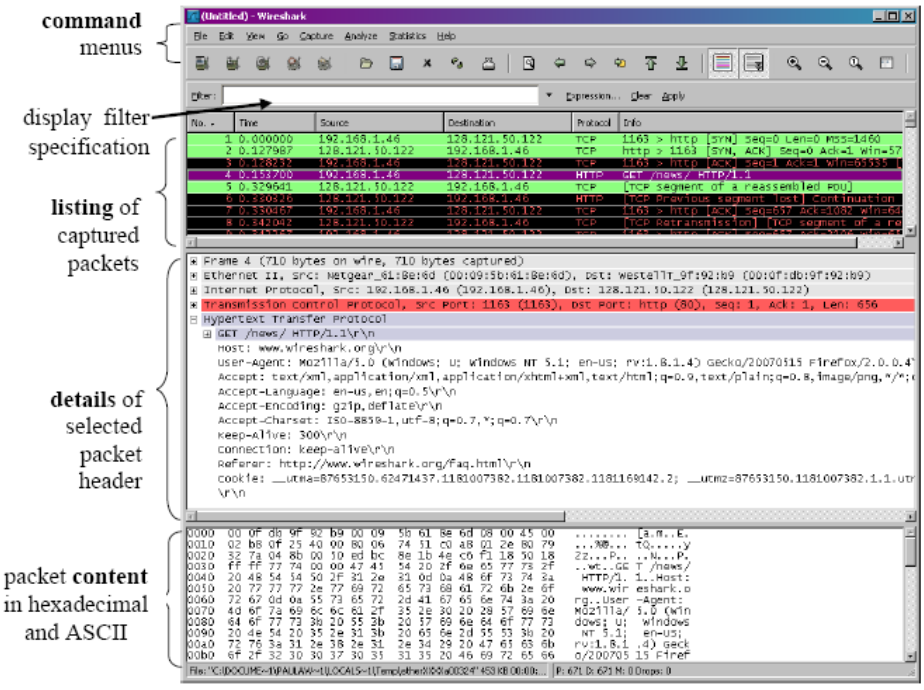

Figura 3. Interface gráfica inicial Wireshark

3. Não pare a captura de pacotes ainda.
4. Enquanto o Wireshark está executando, entre com a URL no seu navegador: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html. Para mostrar esta página, seu navegador fará contato com o servidor HTTP gaia.cs.umass.edu e trocará mensagens HTTP com o servidor para realizar o download desta página para ser mostrada para você. Os quadros Ethernet contendo essas mensagens HTTP serão capturados pelo Wireshark.
5. Depois da página denominada INTRO-wireshark-file1.html ser mostrada no seu navegador, pare a captura de pacotes no Wireshark (selecione "Stop" no menu "Capture"). Na sua lista de pacotes, há todos as mensagens de protocolos trocadas entre seu computador e as outras entidades da rede, inclusive as mensagens de HTTP mencionadas acima.
6. Digite **http** na janela de filtro mostrada abaixo do menu principal do Wireshark. Selecione o botão "Apply". Assim, apenas as mensagens HTTP serão mostradas.
7. Selecione a primeira mensagem HTTP mostrada na lista de pacotes. Ela será a mensagem HTTP GET que foi enviada do seu computador para o servidor HTTP gaia.cs.umass.edu solicitando a página desejada. Quando você seleciona a mensagem, os cabeçalhos de cada camada na mensagem aparecerá.
8. Finalize a execução do Wireshark. Não esqueça de salvar cada execução de suas atividades práticas.

Exercícios

Para você conhecer mais sobre a ferramenta, responda às questões abaixo.

1. Liste os 10 diferentes protocolos que aparecem na coluna de protocolos na lista de pacotes (antes de aplicar o filtro http).
2. Quanto tempo durou de quando a mensagem HTTP GET foi enviada até a resposta HTTP OK ser recebida? (Por default, o valor da coluna *Time* está descrita em segundos, desde que o trace Wireshark iniciou. Você pode mudar da forma que desejar no menu "View", selecionando "Time Display Format").
3. Qual é o endereço IP do servidor gaia.cs.umass.edu? Qual é o seu endereço IP?

"Conte-me e eu esquecerei. Mostre-me e eu lembrarei. Envolva-me e eu compreenderei."
Provérbio Chinês