Missão: Captura de pacotes do tráfego da rede com *Wireshark*.
Recursos: Acesso à Internet e documento PDF com as respostas mínimas, conforme orientação. Oracle Virtual Box. Windows ou Kali Linux. *Wireshark* (download gratuito - diversas plataformas em: http://www.wireshark.org/download.html).
Atividades: Instalação e configuração do software, execução das atividades e preenchimento do formulário do relatório.
Tempo previsto: Duas aulas.

Apresentação:

O *Wireshark* é uma ferramenta para monitorar e analisar trafego de rede. Nesta atividade será utilizada para aprender a identificar o conteúdo deste tráfego.

Antes porém vamos falar sobre o que Wireshark faz. Os softwares deste tipo são chamados de *packet sniffers* (farejadores de pacotes, em tradução livre), e monitoram todos os dados que entram e saem dos dispositivos por meio de interfaces de rede, tal como a placa Ethernet de um computador pessoal ou a interface *wireless* de um notebook.

Pode-se então, dividir o software em duas partes principais, a de captura e a de análise dos pacotes. A primeira (*pcap*) faz uma cópia de todos os frames enviados e recebidos pela camada de enlace. Os pacotes em questão não são - e nem precisam ser - destinados ao *sniffer*. O software em sí é passivo, ou seja, não envia nenhum tipo de pacote: apenas as demais aplicações em execução.

Já a outra parte - análise de pacotes - e mostra de forma fácil ao usuário todos os campos dos pacotes capturados, tanto cabeçalhos quanto dados. Dessa forma é necessário que esta parte do software tenha capacidade de tratar boa parte - senão todos - dos protocolos utilizados, tanto os de aplicação (HTTP, FTP) quanto os das outras camadas (transporte, rede e enlace).

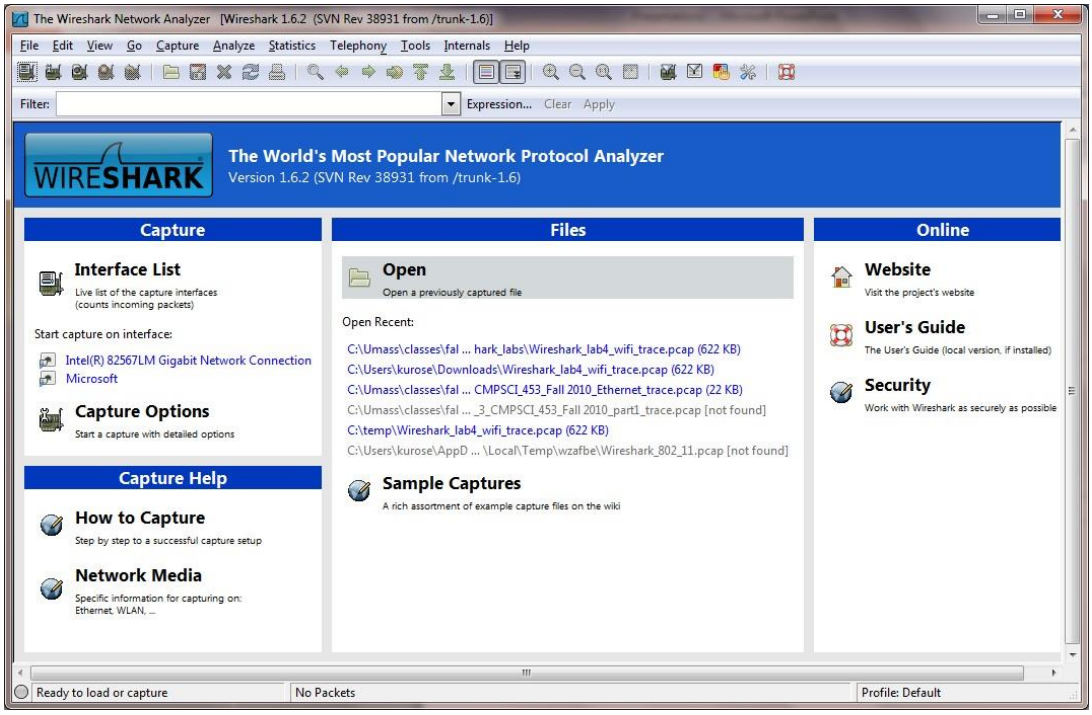

Figura 1: tela inicial de captura do Wireshark

Iniciando o Wireshark, você deverá visualizar a tela inicial do programa, como mostrado na figura 01. Nesta tela é possível, dentre outras coisas, abrir arquivos contendo a captura de pacotes feita previamente (ao centro) e selecionar uma interface para iniciar a captura de pacotes (canto superior esquerdo). Para dar início à captura, selecione a interface utilizada para conectar-se à rede, (a interface sem fio do notebook, se for o caso). Para configurar opções avançadas basta um clique duplo. Para dar inicio à captura selecione a terceira opção da barra de ferramentas. Assim que a captura de pacotes se iniciar, teremos uma exibição na tela conforme mostra a figura 02:

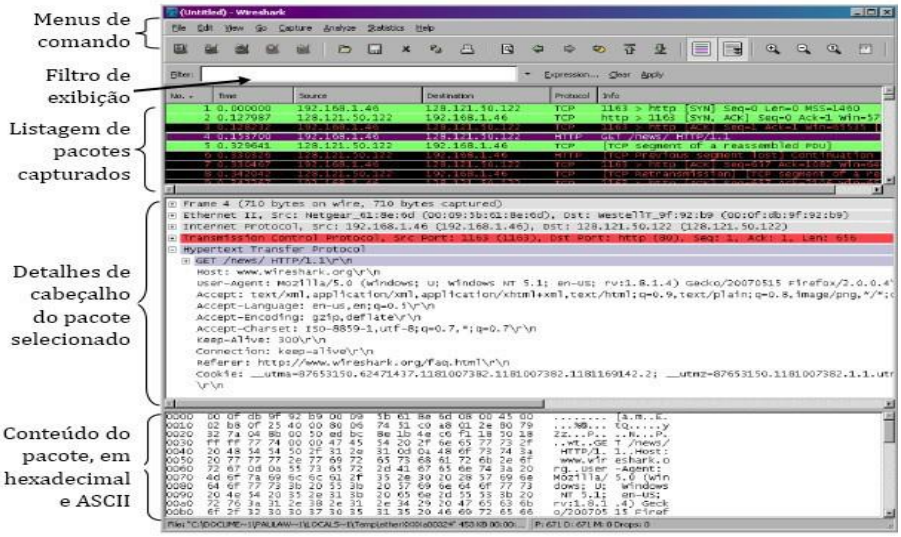

Figura 2 - A tela de captura de pacotes.

A interface do programa apresenta cinco componentes principais:

Menus de comando: ficam no topo da janela e inicialmente é interessante ressaltar o menu *File* e o *Capture*, que nos permitem salvar os pacotes capturados em um arquivo e também iniciar/interromper a captura de pacotes;

Filtro de exibição: filtra a exibição (e não a captura) dos pacotes de acordo com critérios do usuário, como exibir apenas o protocolo FTP, ou pacotes cujo IP de destino seja 8.8.8.8, ou uma combinação de ambos. É importante ressaltar que o filtro é sensível ao caso (difere maiúsculas e minúsculas) e é necessário usar o *Enter* após incluir as regras de filtragem para que o filtro torne-se efetivo.

Janela de pacotes capturados: apresenta a você um resumo de uma linha do pacote (tempo, IP de origem e destino, protocolo utilizado na camada mais elevada, etc.), deixando você ordenar os pacotes por qualquer um desses critérios. Vale a pena ressaltar que a numeração do pacote é própria do Wireshark e se relaciona apenas com a ordem de captura do tráfego. Para selecionar algum pacote basta clicar (botão esquerdo do mouse) sobre ele.

Janela de detalhes do cabeçalho: detalha o conteúdo do pacote selecionado na listagem acima. Exibe informações do cabeçalho desde a camada de enlace - como um frame Ethernet - até a camada de aplicação - como uma requisição HTTP. É possível expandir ou encolher as informações dos cabeçalhos de cada uma das camadas, de acordo com a necessidade.

Janela do conteúdo do pacote: exibe tanto em hexadecimal quanto em ASCII os conteúdos do pacote selecionado. As partes referentes aos cabeçalhos das diferentes camadas são realçados quando selecionados na janela de detalhes de cabeçalho.

Considerando que a interface utilizada é do tipo Ethernet - o recomendado para os primeiros testes do software – vamos às atividades:

1) Acesso o Windows e inicie o *Wireshark*.
2) Acesse o relatório de atividades disponível no link https://goo.gl/forms/FEKw9U4zgUL6ZPQd2) e preencha as informações de identificação. Não o finalize, pois você precisará responder as questões durante a execução da atividade.
3) Inicie o browser no computador.
4) Inicie o *Wireshark* - note que ainda não iniciou a captura de pacotes: você deve ver uma janela como a figura 01.
5) Selecione então a opção *Interfaces* do menu *Capture*. A janela "*Wireshark: Capture Interfaces*" se abrirá, como na figura 03.

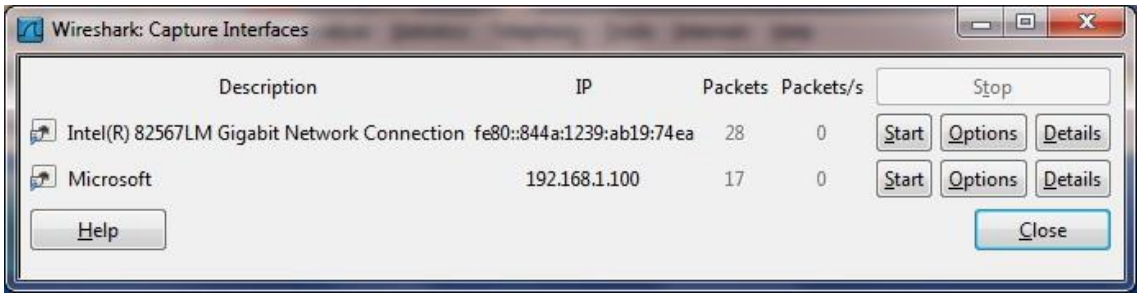

Figura 3: janela Wireshark: Capture Interfaces.

6) Nela estarão relacionadas todas as interfaces do seu computador, com seus nomes, endereços de IP e a quantidade de pacotes observados em cada uma delas. Selecione a interface desejada clicando no botão Start. Agora o Wireshark está capturando todos os pacotes enviados/recebidos pelo seu computador na interface selecionada!
7) Você irá visualizar uma janela como na figura 02, listando todos os pacotes capturados. Vamos então gerar algum trafego interessante para ser analisado, no caso utilizando o protocolo HTTP.
8) Com o Wireshark ainda em execução, acesse no seu browser a seguinte URL: http://gaia.cs.umass.edu/wireshark- labs/INTRO-wireshark-file1.html. Seu computador irá trocar mensagens HTTP com o servidor para fazer o download da página. Os frames Ethernet contendo as mensagens HTTP serão capturadas pelo Wireshark e exibidos na janela de captura.
9) Após a página web ser exibida, interrompa a captura de pacotes acessando o menu *Capture* ou pelo atalho Ctrl+E. O que está sendo exibido na tela é um registro de toda a comunicação feita pelo seu computador com outras entidades na rede, incluindo o servidor responsável por gaia.cs.umass.edu.
10) Como você poderá observar, haverá mais operações acontecendo, além daquelas que decorrem do que você solicitou: a simples ação de acessar uma única página da web.
11) Para filtrar o que desejamos observar, basta inserir na barra do filtro de exibição "http" (sem as aspas). Não se esqueça de clicar em *Apply* (ou pressionar *Enter*). E lembre-se que o campo é sensível ao caso (maiúsculas / minúsculas). Observe agora apenas as mensagens utilizando o protocolo HTTP estão sendo exibidas na janela de exibição de pacotes.
12) Encontre a mensagem HTTP GET que foi enviada do seu computador para o servidor HTTP gaia.cd.umass.edu. Quando o pacote for selecionado os cabeçalhos da frame Ethernet, do datagrama IP, do segmento TCP e da mensagem HTTP serão exibidos na janela de detalhes de cabeçalho. Minimize todas as informações exibidas exceto as do cabeçalho HTTP, então deve- se ter algo semelhante à figura 04 abaixo;
13) Esse é o final da atividade. Na sequência vamos analisar o que realizamos.

Dicas:
O Wireshark não salva automaticamente a captura. Você pode fazer isso selecionando a opção *Save* no menu *File* (atalho Ctrl+S). Selecione o formato do arquivo como .pcap (e não .pcapng) para maior compatibilidade com outros softwares similares. Explore os demais menus do programa, especialmente o menu *Statistics* e familiarize-se com as opções disponíveis.

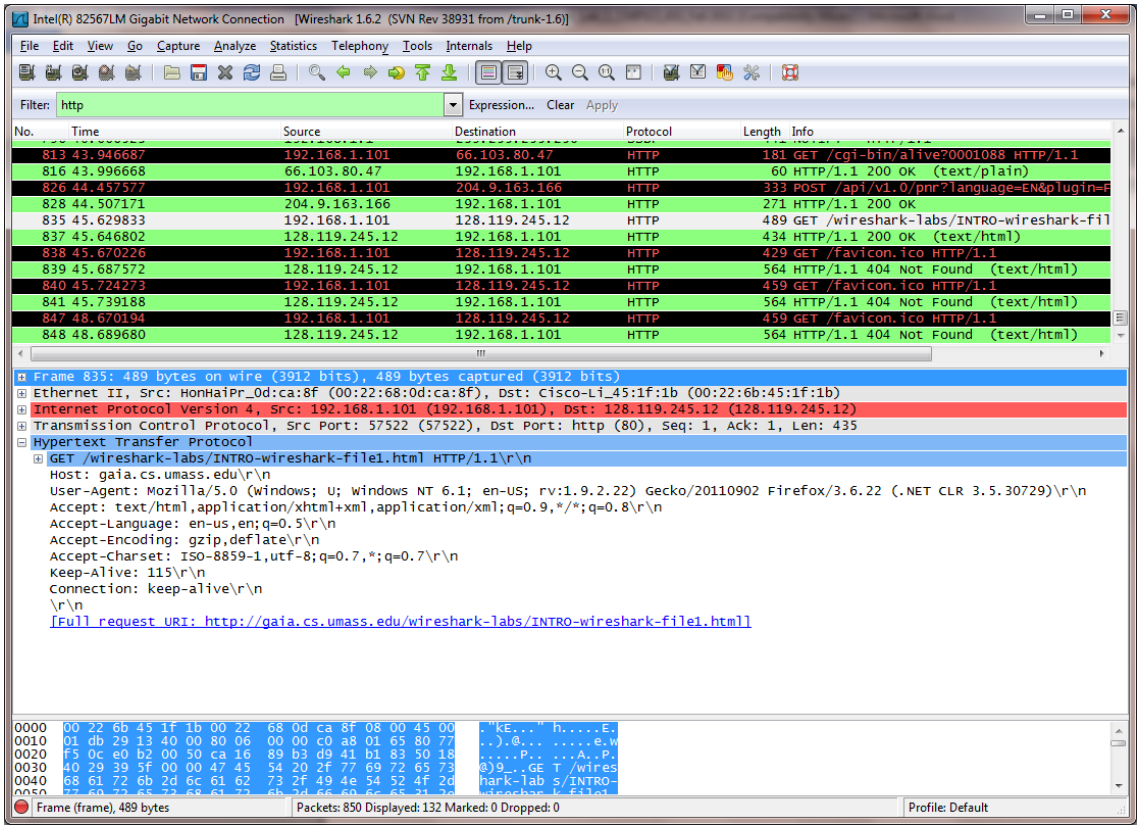

Figura 4: janela do Wireshark após a captura de tráfego HTTP.

14) Agora complete seu relatório de atividades e finalize-o: com base no que foi realizado, responda as seguintes perguntas nos respectivos espaços do Relatório de Atividades:

I. Que outros protocolos podem ser observados na listagem de pacotes com o filtro de exibição desabilitado?

II. Qual o tempo transcorrido entre o envio da mensagem GET e a chegada da resposta HTTP OK? (Por padrão, o tempo exibido na coluna *Time* indica quanto tempo passou desde o início da captura de pacotes. Na opção *Time Display Format*, no menu *View*, é possível alterar a coluna para outros formatos.)

III. Qual é o endereço IP do servidor gaia.cd.umass.edu? Qual o endereço IP do seu computador?

IV. Qual é a porta de destino da mensagem HTTP GET? E a porta de origem?

V. Ainda com o filtro de exibição habilitado como indicado no item 8, selecione a mensagem HTTP GET, vá no menu *View*, selecione a opção *Colorize Conversation* e escolha a cor de sua

preferência. Em seguida, desabilite o filtro de exibição, selecionando *Clear* na mesma barra. Que outros pacotes estão destacados com a cor escolhida? A qual camada de rede eles pertencem e qual a função destes pacotes?

Obs: como sugestão, caso seja necessário imprimir alguns pacotes, selecione *Print* no menu *File* e marque as opções *Selected Packets Only* e *Print as Displayed*.

Referências:

- Supplements: Wireshark Labs, em http://www-net.cs.umass.edu/wireshark-labs/
- Sniff free or die. Em https://blog.wireshark.org/2013/10/switching-to-qt/
- Wireshark: Manual do Usuário, em http://www.wireshark.org/docs/wsug_html_chunked/

A você que se dedica a vencer seus limites e aprender, eu desejo muito sucesso! - Prof. Luis Gonzaga

- e-mail: luis.p@uninter.com
- site: http://www.gonzaga.eti.br/
- blogs: http://verbavitaeaeternae.blogspot.com.br/
  http://gonzagatheblogger.blogspot.com.br/
  http://securitydrivendevelopment.blogspot.com.br/

Mas buscai primeiro o Reino de Deus e a sua justiça, e todas essas coisas vos serão acrescentadas" Mt. 6:33.