Aluno: Diego Silva Cintra RGA: 2012.1904.003-7

Atividade lab04 – Wireshark

1. Liste os diferentes protocolos que aparecem na coluna de protocolo na janela de listagem de pacotes sem a filtragem do passo 7 acima.

R: A filtragem do passo 7 só exibia os protocolos “HTTP”. Sem isso, podemos ver diversos outros protocolos capturados pelo Wireshark, como o SSDP (*Simple service discovery protocol*), baseado no HTTPU - uma extensão do HTTP/1.1 - que utiliza na camada de transporte o protocolo UDP. Temos também, intuitivamente antecedendo o HTPP, a resolução de nomes (DNS) da URL http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html, que possui primeiramente a pergunta (“Standard query”) do usuário para o servidor de DNS e logo em seguida a resposta (“Standard query response”), que envia o “tipo” do site, sua “classe” e seu respectivo endereço (IP). Em seguida, diversos protocolos TCP são vistos, cada um contendo um envio de requisição (sinal “SYN”) de conexão seguido da autorização (sinal “ACK”). Por último, dois protocolos “HTTP” aparecem, com a requisição (“request”) mais seu cabeçalho e a resposta (“response”) do servidor contendo, além de também um cabeçalho, o arquivo “html”.

2. Quanto tempo passou desde que a mensagem GET do http foi enviada até que a resposta OK tenha sido recebida?

R: Analisando a coluna de Tempo, foi-se gasto 0.267369 segundos para o recebimento da resposta.

3. Qual é o endereço Internet de gaia.cs.umass.edu (também conhecido como www-net.cs.umass.edu)? Qual é o endereço IP do seu computador?

R: O endereço IP da máquina cujo teste foi realizado é 192.168.1.2, enquanto que o endereço IP de gaia.cs.umass.edu é 128.119.245.12.

4. Imprima duas mensagens HTTP apresentadas no passo 9 acima.

R: As mensagens, como requisitado, foram impressas em dois arquivos “pdf” separados, inclusos a essas respostas. O arquivo “http_get.pdf” identifica o pacote de requisição do cliente, enquanto “http_ok.pdf” representa a resposta do servidor.

5. Há outras mensagens relacionadas a requisição ao site gaia? Se sim, o que é procurado e qual o retorno?

R: No “HTTP response” (resposta do servidor), temos algumas informações presentes no cabeçalho, como a data de última modificação, qual a aplicação responsável do lado do servidor e o tamanho do arquivo enviado. O campo contendo o arquivo propriamente dito também é exibido. Além disso, alguns protocolos TCP são invocados depois da resposta do servidor, mas infere-se que isso é feito para continuar a conexão caso o cliente venha a requisitar mais páginas do servidor. O retorno desses protocolos, intuitivamente, são os sinais “ACK”.