UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA DE COMPUTAÇÃO E AUTOMAÇÃO

Roteiro de Aula Prática – Introdução ao Wireshark	
DISCIPLINA:	DCA0130 – REDES DE COMPUTADORES
PROFESSOR:	Carlos Manuel Dias Viegas

Esta prática consiste em uma introdução básica ao uso do Wireshark para o estudo das camadas de protocolos do modelo TCP/IP.

- Os requisitos para a realização desta prática são a instalação do *software* Wireshark e ter assistido às videoaulas sobre os modelos de camadas OSI e TCP/IP e sobre o Wireshark disponibilizadas no SIGAA;
- Esta prática consiste em realizar as tarefas descritas abaixo e responder às questões propostas;
- Este documento, com as devidas respostas, deverá ser submetido em uma tarefa específica no SIGAA até o dia **05/11/2021**;
- Esta prática deve ser realizada em duplas, podendo ser formadas por alunos de diferentes turmas da disciplina de redes de computadores (DCA0130) do semestre 2021.2.

Nome do discente (1): Isaac de Lyra Junior Turma: 02

Nome do discente (2): Rodrigo de Lima Santana Turma: 02

Tarefas

1. Iniciar o Wireshark;
2. Escolher a interface de rede que será utilizada para a captura de pacotes;
3. Iniciar a captura e verificar se os pacotes estão sendo de fato capturados;
4. Com o Wireshark ainda em execução e com a captura iniciada, abrir um navegador web e acessar o site www.tribunadonorte.com.br;
5. Parar a captura de pacotes e analisar alguns dos pacotes capturados, observando quais protocolos foram utilizados;
6. Após a análise, aplicar um filtro para apresentar somente os pacotes do protocolo HTTP, digitando: `http` na barra *display filters* (não esquecer de apertar `enter` logo após digitar o filtro);
7. Escolher a primeira mensagem HTTP, que contenha o comando `GET` para o site referido no item 4;
8. Selecionar um dos pacotes HTTP e identificar no painel de detalhes de pacotes:
    a. (Camada 1 - Física) O tamanho em bytes da mensagem: 1106 bytes;
    b. (Camada 2 - Enlace) O endereço MAC de destino 00:e0:4c:c0:e8:86 e de origem a8:5e:45:1e:25:5c;
    c. (Camada 3 - Rede) O endereço IP de destino 23.246.230.134 e de origem 192.168.1.102 ;
    d. (Camada 4 - Transporte) A porta de destino 80 e de origem 38140;
    e. (Camada 5 - Aplicação) Com suas palavras, descreva sucintamente o conteúdo da mensagem:
    Foi feita uma requisição do protocolo HTTP do tipo GET, para o host “www.tribunadonorte.com.br”, contendo as informações de conexão, informações sobre os recursos de suporte, de arquivos e de interpretação, além de cookies e data.

Mensagem:

Hypertext Transfer Protocol

GET / HTTP/1.1\r\n

Host: www.tribunadonorte.com.br\r\n

Connection: keep-alive\r\n

Cache-Control: max-age=0\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n

Referer: http://www.tribunadonorte.com.br/\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: en-US,en;q=0.9,pt-BR;q=0.8,pt;q=0.7\r\n

[truncated]Cookie: _ga=GA1.3.1554731819.1636037965; _gid=GA1.3.616733198.1636037965; __gads=ID=bf4a18a827923bf8:T=1636037966:S=ALNI_MZzBbj3CXbzquHqnd-1mocLdtr3jg; clever-last-tracker-52640=1; _gat_gtag_UA_1869262_3=1; FCNEC=[["AKsRol-KJ-

If-Modified-Since: Thu, 04 Nov 2021 15:07:01 GMT\r\n

\r\n

[Full request URI: http://www.tribunadonorte.com.br/]

[HTTP request 1/1]

[Response in frame: 2731]