|  |  |
| --- | --- |
| http://www.ufc.br/images/_images/a_universidade/identidade_visual/brasao/brasao2_vertical_monocromatico_300dpi.png | **Universidade Federal do Ceará**  **Campus Fortaleza**  **Centro de Ciências Exatas / UFC Virtual**  **Sistemas e Mídias Digitais** |

Disciplina: Rede de Computadores

Professores: Windson Viana

Wireshark – Atividade

**OBJETIVO**

Objetivo dessa atividade é aplicar os conceitos fundamentais de Redes de Computadores dos capítulos 1, 2, 3, 4 do Kurose utilizando o software Wireshark. Você pode ver um material introdutório de Wireshark [clicando aqui](https://docs.google.com/document/d/1BBwz7Dzeo3H49AS7bbCr_C1gtGUX5LS5Yp2xJZDoBIE/edit?usp=sharing).

**ATIVIDADE**

|  |
| --- |
| Antes de iniciar a atividade realize as seguintes operações |
| Na atividade, vamos capturar os pacotes **DNS** **e HTTP** que são gerados em sua máquina. **O ideal** é que você realize alguns procedimentos para capturar o comportamento esperado  **Exemplos de Procedimentos:**  • Use ipconfig /flushdns para esvaziar o cache DNS em sua máquina.  • Inicie seu navegador e esvazie o cache do navegador.  • Execute Wireshark e digite “ip.addr == seu\_endereço\_IP” no campo de filtro, onde você  obtém o endereço do computador que está executando Wireshark com ipconfig. Este filtro  remove todos os pacotes que não foram originados ou destinados para seu host.  **Atenção: anexe imagens da captura as suas respostas.** |

|  |
| --- |
| **Primeira Captura** |
| Inicie captura de pacotes no Wireshark.  Com seu navegador, visite o site **http://www.virtual.ufc.br**  Finalize a captura de pacotes |

Com base nas informações colhidas responda os itens a seguir.

**Endereçamento IP e Ethernet**

1. Qual é o endereço IP da sua máquina? Qual o endereço IP do servidor HTTP que hospeda a página www.virtual.ufc.br? Qual é o endereço IP do servidor DNS que respondeu à requisição DNS?
2. Qual o endereço físico (MAC Address) da sua máquina? Porque não é possível obter o endereço físico da máquina do servidor da UFC Virtual a partir do Wireshark?

|  |
| --- |
| **Segunda Captura** |
| Inicie captura de pacotes no Wireshark.  Com seu navegador, visite o site <http://pudim.com.br/>  Finalize a captura de pacotes |

**HTTP**

1. a) Quais os protocolos utilizados nas camadas de enlace, rede, transporte e aplicação para obtenção da página do Pudim?

b) Explique porque o HTTP usou o protocolo TCP para transporte

1. Quantas requisições HTTP foram feitas pelo navegador para conseguir baixar por completo a página?
2. Selecione aquela requisição que solicitou o imagem do pudim. Destaque quais são os parâmetros utilizados na requisição GET do HTTP.
3. Qual é o USER AGENT do seu navegador nessas requisições?

**DNS**

1. Em relação à conexão DNS para resolver a requisição <http://pudim.com.br/>, responda:

Qual máquina respondeu à requisição DNS? Em que porta?

Qual foi o(s) endereço(s) IP fornecido(s) como resposta?

Qual era seu Tipo (e.g., MX, A, AAAA)? O que isso significa?

Qual foi o protocolo da camada de transporte utilizado para a requisição DNS do domínio? Explique porque a hierarquia DNS usa esse tipo de protocolo

1. Inicie uma nova captura do Wireshark e acesse o mesmo site novamente sem esvaziar o cachê.
2. No caso do <http://pudim.com.br/>, o que ocorreu de distinto com relação à requisição e a resposta do HTTP?
3. No caso do site da UFC, o que ocorreu de distinto com relação à requisição e a resposta do DNS?

|  |
| --- |
| Terceira Captura |
| Inicie uma NOVA captura no Wireshark.  Efetue um PING na linha de comando para o domínio [www.fifa.com](http://www.fifa.com). Após a execução, execute o traceroute (tracert no windows) para o domínio [www.fifa.com](http://www.fifa.com). Por fim, encerre a captura do Wireshark. Selecione os pacotes ICMP e responda: |

**IP e ICMP**

1. Sobre o PING e Traceroute, responda

Qual é o tamanho dos pacotes enviados no PING?

Qual foi a diferença dos pacotes enviados pelo PING e pelo Traceroute com relação ao campo de endereço de destino?

O que são os pacotes “Time-To-Live exceed”?

1. Faça uma tabela com os ips de origem e destino dos pacotes “echo” e seus respectivos TTL.

Qual é a relação do TTL e a rota do traceroute?

Quais campos no datagrama IP sempre mudam de um datagrama para um outro datagrama, dentro da série de mensagens ICMP enviadas pelo seu computador no traceroute? Quais campos permanecem constantes?