|  |  |
| --- | --- |
| 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**  **Mestrado e Doutorado em Ciência da Computação**  **Sistemas e Mídias Digitais** |

Disciplina: Sistemas Distribuídos

Professores: Fernando Trinta, Windson Viana

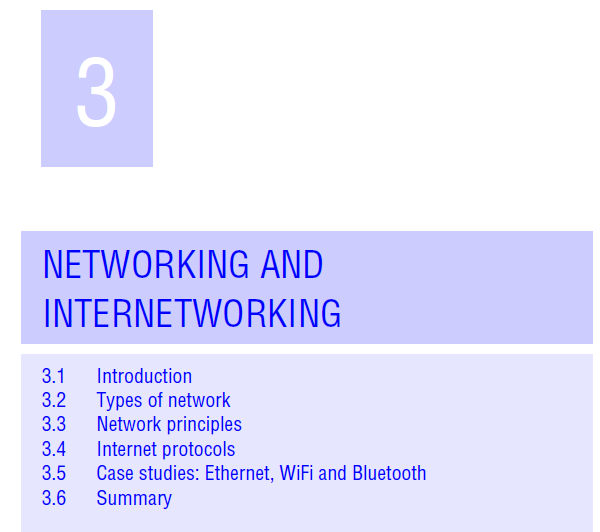
Programa de Estudos de Fundamentos de Redes de Computadores – Sala Invertida

Objetivo do documento: Visa indicar uma sugestão de percurso de estudo sobre os Fundamentos de Redes Computadores

1- Sugestão de Leitura

O conteúdo de Redes de Computadores é pré-requisito fundamental para o entendimento de vários conceitos chaves de sistemas distribuídos tais como as abstrações de middlewares de comunicação (como o Websocket), a invocação de métodos e procedimento pela rede, o funcionamento de Serviços Web e o funcionamento das arquiteturas P2P. Desta forma, esse estudo dirigido visa recapitular pontos chaves do conteúdo de rede, sendo estes: o funcionamento das camadas TCP/IP, o endereçamento IP, as diferenças de funcionamento entre os sockets TCP e UDP, o funcionamento do TCP e os protocolos da camada de aplicação HTTP e DNS.

Esse conteúdo é abordado pelo capítulo 3 do livro de Sistema Distribuídos do Coulouris, disponível na biblioteca da UFC



Para testar seus conhecimentos, você pode acessar esse quiz básico de avaliação do conteúdo: <https://goo.gl/forms/qWFf6G6COwZsNmTE3>

2- Sugestões de Vídeos

Sobre os assuntos chave do capítulo, sugerimos a seguinte lista de vídeos

|  |  |  |
| --- | --- | --- |
| Tema | Links | ~Duração |
| Internet e TCP/IP | <https://www.youtube.com/watch?v=HNQD0qJ0TC4>  <https://www.youtube.com/watch?v=9ndoxFjYqPs>  <https://www.youtube.com/watch?v=W6eB6LoxTNE>  <https://www.youtube.com/watch?v=oz8gvGIUKFw> | 6 min  2 min  13 min  19 min |
| DNS | <https://www.youtube.com/watch?v=NHSepKUCXsk>  <https://www.youtube.com/watch?v=ACGuo26MswI> | 5 min  7 min |
| HTTP | <https://www.youtube.com/watch?v=fhAXgcD21iE>  <https://www.youtube.com/watch?v=SzSXHv8RKdM> | 4 min  9 min |
| TCP vs UDP | <https://www.youtube.com/watch?v=Vdc8TCESIg8> | 12 min |
| Endereçamento IP | <https://www.youtube.com/watch?v=rnV1bD5WUME>  <https://www.youtube.com/watch?v=qbA_n631yAU> | 15 min  13 min |
| Introdução ao Wireshark | <https://www.youtube.com/watch?v=C3epfFoKoFs> | 8 min |
| Exemplos de Análise | <https://www.youtube.com/watch?v=6bRqTkNKbF8>  <https://www.youtube.com/watch?v=RYCH7-PfJpY> | 10 min  7 min |

3- Quiz para análise dos conhecimentos

Os dois quizes dos links abaixo são avaliações formativas que permitem aferir qual é o seu nível de conhecimento quanto aos aspectos abordados no livro texto e nos vídeos.

Você precisa utilizar um email do gmail válido e pode alterar suas respostas quantas vezes desejar. É possível checar quais questões você acertou e quais errou após o preenchimento completo dos formulários.

|  |  |
| --- | --- |
| Tema | Link |
|  |  |
| HTTP e DNS | <https://goo.gl/kbabUv> |
| TCP/IP e Wireshark | <https://goo.gl/forms/Zdfnn1irgOz2JtaP2> |

4- Prévia Inicial da Atividade a ser **Realizada em Sala de Aula**

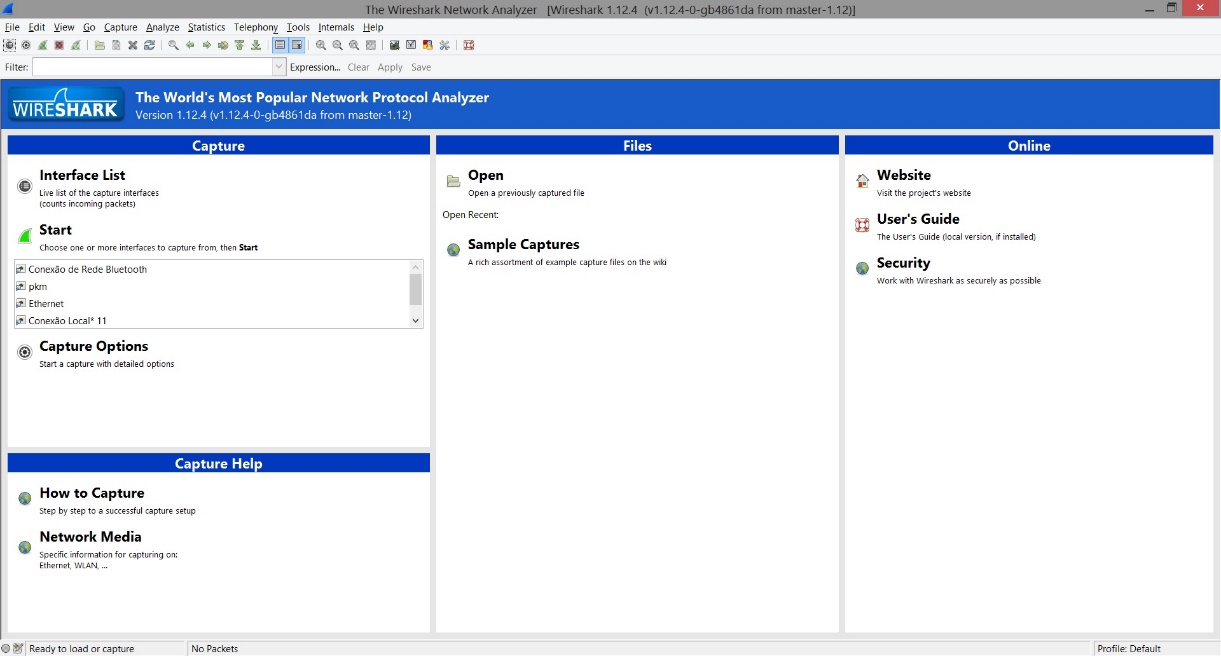
Atividade em Sala de Aula: utilizaremos o Wireshark para identificar as camadas do TCP/IP, comparação do uso de UDP vs TCP, entendimento das requisições HTTP e DNS.

Prática Wireshark – Revisão de Redes

Objetivo da prática é revisar conceitos fundamentais de redes de computadores dos capítulos 1, 2, 3, 4 do Kurose.

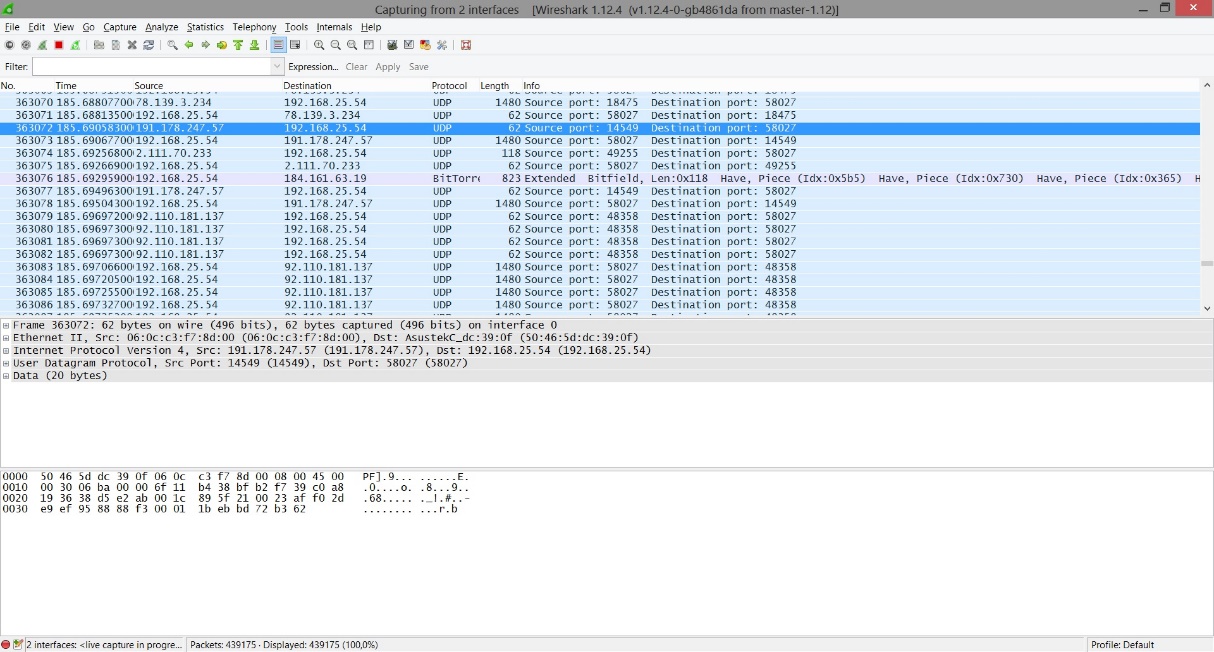
**Aquecimento**

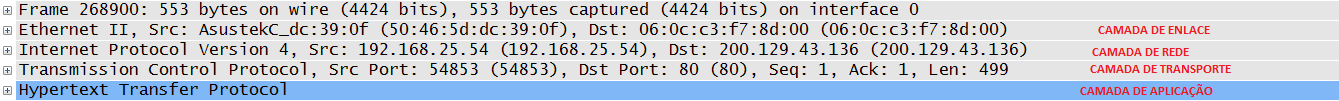
Faça o login nas máquinas e inicie um navegador a sua escolha, em seguida, inicie o programa desktop do Wireshark. Você verá a tela inicial do Wireshark, semelhante a imagem seguinte



À esquerda, selecione todas as opções (as interfaces de captura) e clique em “Start”, logo acima.

O programa lhe levará a uma tela semelhante a esta com os pacotes capturados, ao selecionar um pacote é possível ver o seu conteúdo dividido em cinco camadas



É possível ver os pacotes que estão sendo trocados pela rede, assim como os protocolos utilizados em cada camada. O programa nos também permite filtrar os protocolos visíveis no log

Mais informações sobre o Wireshark

|  |  |  |
| --- | --- | --- |
| Tema | Links | **~Duração** |
| Introdução ao Wireshark | <https://www.youtube.com/watch?v=C3epfFoKoFs> | 8 min |
| Exemplos de Análise | <https://www.youtube.com/watch?v=6bRqTkNKbF8>  <https://www.youtube.com/watch?v=RYCH7-PfJpY> | 10 min  7 min |

**Ipconfig**

Ipconfig (para Windows) e ifconfig (para Linux/Unix) estão entre as mais úteis ferramentas, especialmente para “debugar” questões da rede. Vamos descrever somente o ipconfig (muito parecido com o ifconfig) nesta aula prática. Ipconfig pode ser usado para mostrar a informação atual TCP/IP, incluindo seu endereço IP, endereço de servidor DNS, tipo de adaptador e etc. Por exemplo, se você deseja ver as informações sobre seu host, simplesmente digite no prompt do Windows: ipconfig /all ipconfig é também muito útil para gerenciar a informação DNS armazenada no host. Para ver os registros armazenados em cache, digite o seguinte comando: ipconfig /displaydns

**ATIVIDADE**

|  |
| --- |
| Antes de iniciar a atividade realize as seguintes operações |
| Vamos capturar os pacotes DNS **e HTTP** que são gerados. **Mas antes:**  • 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.  • 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. **Atenção: anexe imagens às suas respostas.**

1. Identifique o endereço IP da máquina que você está utilizando e do servidor da página (listados nas colunas “source” e “destination”).
2. Identifique as consultas DNS feitas para encontrar o endereço (filtre por “dns” em vez de “http”).

**Endereçamento IP e Ethernet**

1. Qual o endereço IP da sua máquina? Qual o endereço IP do servidor da página www.virtual.ufc.br? Qual o endereço IP do servidor DNS que respondeu a requisição DNS?
2. Qual o endereço físico (MAC Address) da sua máquina? É possível obter o endereço físico da máquina do servidor?

**HTTP**

1. Quais os protocolos utilizados nas camadas de enlace, rede, transporte e aplicação para obtenção da página do Instituto?
   1. Explique porque o HTTP usou o protocolo TCP para transporte
2. Quantas requisições HTTP foram feitas pelo navegador para conseguir baixar por completo a página do instituto?
3. Selecione aquela requisição que solicitou o logo.png da página. Destaque quais são os parâmetros utilizados na requisição GET do HTTP.
4. Qual é o USER AGENT do seu navegador nessas requisições?
5. Ao selecionar a resposta da requisição do logo.png é possível verificar na mensagem respondida, algumas informações sobre PNG. Por exemplo, cite qual foi a sua data de modificação e qual foi o software utilizado para sua construção.

**DNS**

1. Selecione as requisições e respostas da hierarquia DNS sobre o portal da UFC Virtual.
   1. Qual máquina respondeu à requisição? Em que porta?
   2. Qual foi o(s) endereço(s) fornecido(s) como resposta?
   3. Qual era seu Tipo? O que isso significa?
   4. 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
   5. A requisição TCP realizada para requisitar a página usou qual IP como destino (pacote TCP SYN)? Ele estava listado na resposta DNS?
2. Inicie uma nova captura do Wireshark e acesse o mesmo site novamente sem esvaziar o cachê.
   1. O que ocorreu de distinto com relação à requisição e a resposta do HTTP?
   2. O que ocorreu de distinto com relação à requisição e a resposta do DNS?

**IP e ICMP**

|  |
| --- |
| Antes de iniciar **ess**a atividade realize as seguintes operações |
| **Inicie uma NOVA captura no Wireshark.**  **Efetue um PING para o domínio** [**www.fifa.com**](http://www.fifa.com)**. Após a execução, execute o tracert para o domínio** [**www.fifa.com**](http://www.fifa.com)**. Por fim, encerre a captura do Wireshark. Selecione os pacotes ICMP e responda:** |

1. Qual é o tamanho dos pacotes enviados no PING?
2. Qual foi a diferença dos pacotes enviados pelo PING e pelo Traceroute?
3. O que são os pacotes “Time-To-Live exceed”?
4. 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?
5. É possível saber se houve fragmentação dos pacotes? Como?
6. Quais campos no datagrama IP sempre mudam de um datagrama para o outro dentro da série de mensagens ICMP enviadas pelo seu computador no traceroute? Quais campos permanecem constantes?

**DHCP**

|  |
| --- |
| Antes de iniciar **ess**a atividade realize as seguintes operações |
| **1. Vá na linha de comando e execute ipconfig /release. Esse comando removerá a configuração de ip atual da sua máquina**  **2.** Inicie o sniffer de pacotes Wireshark e começ**e** a captura de pacotes Wireshark.  3. Agora, volte ao prompt de comando do Windows e digite “ipconfig / renew”.Isso instrui seu host a obter uma configuração de rede, incluindo um novo IPendereço **por meio do DHCP**.  4. Aguarde até que o “ipconfig / renew” tenha terminado. Em seguida, digite o mesmo comando  “Ipconfig / renew” novamente.  **5**.Quando o segundo “ipconfig / renew” terminar, digite o comando  “Ipconfig / release” para liberar o endereço IP atribuído anteriormente ao seu computador.  6. Por fim, insira “ipconfig / renew” para receber novamente um endereço IP para seu  computador.  **7.** Pare a captura de pacotes Wireshark.  **8. Selecione os pacotes DHCP usando o filtro (“bootp” ou “dhcp”)** |

1. Identifique quais foram os pacotes enviados e recebidos do protocolo.

a) Quantos servidores DHCP responderam?

* 1. Quais endereços IPs (origem e destino) foram usados pelo seu computador para achar o servidor DHCP pela primeira vez?

1. Qual mensagem contém as informações necessárias para configuração da sua máquina?
2. Porque no segundo “renew” não foram enviadas mensagens Discover e nem recebidas mensagens Offer?
3. Houve diferenças nas duas mensagens de Discover enviadas?
4. Descreva a função da mensagem Release.

Discussão e Reflexão em Grupo

1. (Segurança vs Desempenho) A quantidade de informação que trafega sem criptografia na Internet é suficiente para descobrir sobre o comportamento de um usuário na rede? Por que não usar HTTPS ou SSL para essas requisições?
2. (Tráfego não gerado pelo usuário) O que são os protocolos QUIC e SSDP e porque tanto tráfego desses pacotes está sendo capturado? É possível reduzir a transmissão desses pacotes?
3. O que comportamento da Rede ou dos protocolos que mais o surpreendeu com o uso do Wireshark?