

Wireshark

Exercício 01. Abra o arquivo [exercicio-um.pcap](#). Você deverá ver 26 pacotes nesse arquivo. O conjunto de pacotes descreve uma “conversa” entre usuários clientes e um servidor central. Toda essa conversa acontece automaticamente depois que um usuário digita algo e tecla enter. Analise os pacotes para responder às seguintes questões em relação a essa conversa.

- a) Qual é o endereço IP do cliente que inicia a conversa? **R= 131.247.95.216**
- b)** O que está ocorrendo nos frames 3, 4 e 5? **R= A sincronização iniciada: O cliente solicita permissão ao destino inicio da conversa, logo em seguida o servidor responde afirmativamente. O cliente envia um pacote marcado com "ACK" e a conexão está estabelecida entre cliente e servidor.**
- c)** O que está ocorrendo nos frames 6 e 7? **R= O cliente está solicitando a página web e o servidor confirma este pedido.**
- d) Ignore o frame 8. Contudo, para sua informação, o frame 8 é utilizado para gerenciar o controle de fluxos.
- e) O que está ocorrendo com os frames 9 e 10? **R= O servidor fragmentou os pacotes de dados da página web não enviando toda a informação de uma vez. Em seguida o servidor envia a mensagem que transferiu toda a informação.**
- f)** O que está ocorrendo no pacote 11? **R= O cliente confirma o recebimento dos pacotes (text/html).**
- g) Após o recebimento do primeiro conjunto de pacotes, o cliente envia uma nova solicitação no pacote 12. Isso ocorre automaticamente sem qualquer ação realizada pelo usuário. Por que isso ocorre? **R= Na última ação foram transferidos os pacotes em formato texto. Posteriormente são transferidos, no pacote 12, os arquivos de imagem que constituem a página.**
- h) O que está ocorrendo nos pacotes 13 a 22? **R= O servidor fragmentou o arquivo de imagem, e envia ao cliente em vários segmentos. No pacote 22 envia uma mensagem ao cliente confirmando o envio de todo o arquivo.**
- i)** Explique o que está ocorrendo nos pacotes 23 a 26. **R= O cliente solicita um arquivo de imagem (favicon.ico). O servidor fragmenta e envia o arquivo. Manda mensagem com OK. O cliente confirma o recebimento do arquivo.**
- j)** Em poucas palavras descreva o que o usuário está fazendo (lendo email? Acessando uma página web? FTP? Outro?) **R= O usuário está acessando a página web <http://www.google.com.br>**

Exercício 02. Abra o arquivo [exercicio-dois.pcap](#). Você deverá ver 176 pacotes listados.

- a) Nos primeiros pacotes, a máquina cliente está procurando o *common name (cname)* de uma página web para encontrar o seu endereço IP. Qual o *cname* desta página web? Cite dois endereços IP desta página web. **R= 216.109.117.106; 216.109.117.109**
- b) Quantos pacotes/quadros são necessários para receber a página web (referente apenas ao primeiro http request)? **R= 17**
- c) O que está ocorrendo nos pacotes 26 e 27? Todos os componentes de uma página web tem de vir de um mesmo servidor? Dica: Seu computador usa um pedido de DNS para pesquisar um CNAME e ele retorna um conjunto de endereços IP (um endereço

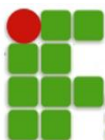
primário e um ou mais endereços de backup) que podem ser usados para entrar em contato com o servidor. **R= Um arquivo de imagem do site está hospedado em outro endereço. Nesse caso o cliente solicita esse endereço ao servidor.**

- d) No pacote 37 vemos outra consulta DNS, desta vez para us.i1.yimg.com. Por que o cliente precisa pesquisar sobre esse endereço IP? Não obtivemos este endereço no pacote 26? (Compare cuidadosamente os dois nomes comuns nos pacotes 26 e 37.) **R= Os domínios são diferentes, basta ver que us.js2.yimg.com é diferente de us.i1.yimg.com e para cada um deles temos um endereço IP diferente.**
- e) No pacote 42 vemos uma declaração HTTP "Get" e, no pacote 48, uma nova declaração HTTP "Get". Por que o sistema não precisa de outro pedido de DNS antes da segunda declaração de obtenção? Clique no pacote 42 e olhe na janela do meio. Expanda a linha intitulada "Hypertext Transfer Protocol" e leia a linha "Host:". Compare essa linha com a linha "Host:" para o pacote 48. **R= Os 2 arquivos pertencem ao mesmo domínio (us.yimg.com/i/ww)**
- f) Examine o pacote 139. Este é um segmento de uma PDU que é remontado com vários outros segmentos no pacote 160. Olhe para os pacotes 141, 142 e 143. Esses três pacotes também fazem parte do pacote 160? O que acontece se um conjunto de pacotes que deveriam ser remontados não chegam em um fluxo contínuo ou não chegam na ordem correta? **R= Não fazem parte do pacote 160 os pacotes 141 e 142. O pacote 143 faz parte do pacote 160.**

Exercício 03. Abra o arquivo [exercicio-tres.pcap](#). Você deverá ver 22 pacotes listados. Esses pacotes representam duas diferentes solicitações de acesso a páginas web. Pacotes 1-7 dizem respeito a solicitações da página yahoo.com, enquanto que os pacotes 8-22 dizem respeito a página my.usf.edu.

- a) Compare a porta de destino no pacote TCP no quadro 3 com a porta de destino no pacote TCP do frame 12. Qual diferença você pode notar? O que isso diz sobre a diferença entre as duas solicitações? **R= Os destinos são diferentes. A porta 80 do pacote 3 se refere ao protocolo HTTP, já a porta 443 do pacote 12 se refere ao HTTPS (Hyper Text Transfer Protocol Secure - protocolo de transferência de hipertexto seguro).**
- b) A tabela a seguir compara os dois pedidos para as páginas web. Por exemplo, a linha i) mostra que quadros 1-2 e quadros 8-9 representam as pesquisas de DNS para cada uma das solicitações

Linha	quadro yahoo.com	quadros my.usf.com	Breve explicação da atividade
i)	1-2	8-9	Solicitação DNS para buscar o endereço IP para CNAME & Resposta DNS
ii)	3-5	10-12	Three-way handshake
iii)	--	13-20	
iv)	6	21	Solicitação GET



v)	7	22	Primeiro pacote do servidor web com o conteúdo da página web;
----	---	----	---

Explique o que está acontecendo na linha iii. Por que não existem quadros listados para yahoo na linha iii? **R= o Protocolo HTTPS criptografa os dados da página, dessa forma os dados do quadro não são mostrados.**