CES-35 – Redes de Computadores e Internet

**Laboratório número 1**

**Conhecendo protocolos - Wireshark**

Em seu relatório siga rigorosamente o roteiro abaixo. Inclua as perguntas na ordem em que aparecem seguidas das respectivas respostas. Não precisa introdução nem conclusão.

1. Inicie o seu navegador (browser). Inicie o Wireshark e selecione a interface onde vai capturar pacotes que deve ter acesso a Internet. Inicie a capture (Start).
2. Acesse a URL do site do Kurose: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html no navegador. Pare a captura (Stop).

Você pode salvar esta captura para ir respondendo as perguntas abaixo em diferentes momentos. Para salvar File→ Save as → salve no formato próprio do wireshark que usa a biblioteca pcapng. Não se esqueça de outras vezes que tiver que trabalhar com esta mesma captura de abri-lo.

1. Responda as **perguntas gerais**:

3.A) Quais destes protocolos aparecem na lista de pacotes: TCP, QUIC, HTTP, DNS, UDP, TLS?

Se você não viu o protocolo DNS na lista, talvez a requisição necessária não foi feita pois já estava no seu cache. Esvazie o cache de seu browser e recomece do start da captura (Passo 1).

3.B) Quanto tempo transcorreu desde quando a mensagem HTTP GET foi enviada até quando a resposta HTTP OK foi recebida? Observação: Por padrão, o valor da coluna “Time” (na janela de listagem de pacotes capturados) é a quantidade de tempo que passou (em segundos) desde que a captura de pacotes começou. Para exibir a hora do dia na coluna “Time”, selecione a opção “Time Display Format” do menu “View” e, em seguida, selecione a opção “Time-of-day” no menu emergente. Tempo decorrido: \_\_\_\_\_\_\_\_\_

3.C) Aponte para a mensagem que tem o GET e expanda a porção HTTP da mensagem. Olhando os detalhes do pacote, qual a utilidade do campo User-Agent? E na resposta, o que significa o campo Server?

3.D) Aponte para a mensagem que tem o OK, ou seja, a resposta do HTTP GET.

Escreva aqui o tamanho em bytes do cabeçalho de cada camada:

Num. de Bytes do cabeçalho de Aplicação (HTTP):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Num. de Bytes do cabeçalho de Transporte (TCP):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Num. de Bytes do cabeçalho de Rede (Internet Protocol):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Num. de Bytes do cabeçalho de Enlace (Ethernet):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Assim, o total do número de bytes dedicados aos cabeçalhos foi \_\_\_\_\_\_\_\_\_\_.

Dados “úteis”carregados pela resposta ( a página de resposta): \_\_\_\_\_\_\_\_\_\_\_\_\_

Portanto, do total de bytes transferidos nesta mensagem, quanto se refere aos dados úteis em porcentagem? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3.E) Inclua no relatório o print das mensagens HTTP (GET e OK) referentes ao acesso feito em (3). Para isso, no wireshark selecione as mensagens, seleciona File→ Print, selecione “Selected Packet Only” e “All expanded” para que eu possa conferir os campos a que você se refere.

3.F) Defina um filtro no campo de filtro da tela principal do wireshark para observar apenas as mensagens que vêm do IP do site do kurose (ip.addr==xxx.xxx.xxx.xxx). Em seguida, acesse novamente a mesma página citada no item (2) do roteiro.

Você deve obter um pacote de resposta do tipo HTTP 1.1/304 Not Modified. Explique do que se trata. O que fazer para evitar esta mensagem e ter a página transferida novamente? Faça isso.

4. Para estudar superficialmente a **Camada de Transporte**, selecione a mensagem com o GET novamente e responda:

4.A) Expandindo a porção TCP, qual o número da porta de destino para o qual a requisição HTTP foi enviada? Porta de destino: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E qual o número da porta de origem? Porta de origem: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4.B)Liste o nome dos campos da camada TCP que encontrou neste pacote: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4.C) Os protocolos criam sua maneira de conversar, por exemplo, através de bits ligados nas mensagens trocadas, os chamados flags. Há pacotes de controle do TCP que não carregam dados de aplicação. Estão nesta categoria 3 pacotes TCP anteriores ao pacote do HTTP GET. Estes pacotes formam o chamado 3-way handshake e são usados para estabelecer a conexão com o outro lado antes de fazer a requisição propriamente dita. Este handshake envolve os flags SYN e ACK no cabeçalho. Encontre 3 pacotes anteriores ao GET que usam as mesmas portas do item (5A). Em ordem do menor tempo para o maior. Preencha:

Flag(s) de controle ligado(s) no primeiro pacote do handshake:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Flag(s) de controle ligado(s) no segundo pacote:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Flag(s) de controle ligado(s) no terceiro pacote: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Você vai entender melhor este mecanismo quando estudarmos o nível de transporte, por enquanto basta saber que há diversos pacotes trocados para controlar a conversa.

4.D) No pacote HTTP OK quais são as portas envolvidas?

Porta de origem: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Porta de destino: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4.E) Depois da transferência da página normalmente acontece a desconexão que envolve os flags FIN e ACK. Há pacotes ligados as mesmas portas do item (5A) com o bit FIN? Mencione o instante de tempo, os pacotes e os flags ligados nos pacotes encontrados depois da transferência.

1. O comando ifconfig (Linux) traz os endereços das suas interfaces de rede. Coloque aqui a saída do ifconfig. No Windows o comando equivalente é ipconfig.
2. Para estudar superficialmente a **Camada de Rede**, selecione a mensagem com o GET novamente e responda:

6.A) Endereço IP de gaia.cs.umass.edu : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Endereço IP de seu computador: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6.B)O campo inet na saída do ifconfig é o mesmo do endereço IP que o wireshark mostrou? Espero que sim, pois o Sistema Operacional usa esta configuração ligada a sua placa de rede na hora de montar os pacotes que emite para a rede.

6.C) Liste o nome dos campos da camada IP que encontrou neste pacote: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Para estudar superficialmente a **Camada de Enlace**, selecione a mensagem com o GET novamente. Na camada de enlace os endereços não se referem ao endereçamento mundial IP, mas ao endereço de sua placa de rede que será usado localmente. Responda:

7.A) Endereço MAC de origem: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Endereço MAC de destino \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7.B) Liste o nome dos campos da camada MAC que encontrou neste pacote: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7.C) O campo ether na saída do ifconfig é o mesmo do endereço de origem que o wireshark mostrou? Espero que sim, pois o Sistema Operacional usa esta configuração de sua placa de rede na hora de montar os pacotes que emite para a rede.

Note como, com um simples GET quanta coisa você aprendeu da relação entre os protocolos!

1. Faça um traceroute para o site do Kurose que está no item (2) acima.

(a) Quantos saltos foram necessários até chegar lá?

(b) Há algum passo que tem o valor de tempo menor que o passo anterior? Porque isto aconteceria?

Inclua a saída do traceroute no relatório.