TRABALHO PRÁTICO WIRESHARK

Orientações sobre a atividade prática.

O objetivo desse trabalho é avaliar a sua capacidade de identificar e caracterizar aspectos práticos de Redes de Computadores relacionados aos conteúdos da disciplina por meio de software de análise do tráfego da rede (Será utilizado o Wireshark). Você deve acessar um site, captura os dados da rede por meio do Wireshark e depois gravar um vídeo com as análises da captura conforme as orientações desse documento.

O Wireshark é software gratuito (licença GNU) que é conhecido como um analisador de pacotes de rede (também conhecido como um farejador de pacotes - sniffer). É uma ferramenta capaz de interceptar, registrar e exibir o tráfego que passa através de uma rede (que é capturado pelas placas ou interfaces de rede).

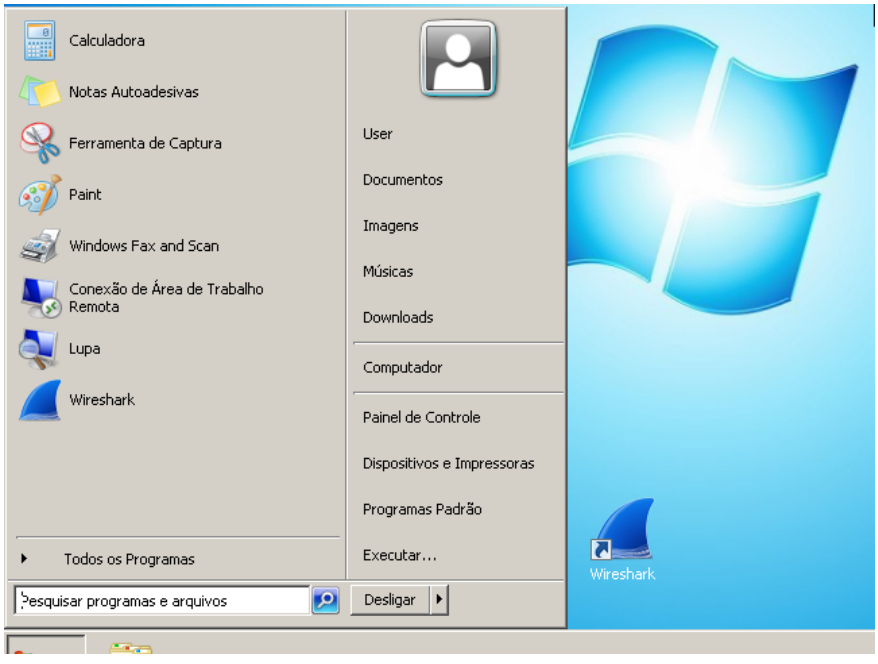
Sniffers como Wireshark podem ser usados para uma variedade de finalidades positivas...
• Analisar os problemas da rede e testar a comunicação da rede;
• Debugar comunicação cliente/servidor e outras comunicações de protocolo de rede;
• Monitorar o uso da rede e largura de banda (incluindo usuários e sistemas internos e externos);
• Detectar mau uso da rede por usuários internos e externos;
• Detectar tentativas de intrusão de rede (como port scanning);
• Filtrar conteúdo suspeito no tráfego da rede.
E negativas...
• Obter informações para efetuar a intrusão de rede;
• Espionar sobre outros usuários da rede e coletar informações confidenciais, como senhas, números de matrícula, documentos, etc (caso criptografia não esteja sendo utilizada para transmissão de determinados tipos de dados).

Nós utilizaremos o Wireshark com o objetivo de olhar mais de perto os protocolos de comunicação de redes.

O Wireshark é gratuito e compatível com todas as máquinas Windows, Mac e Linux / Unix.
Ele pode ser obtido pelo link:
https://www.wireshark.org/download.html

AVISO IMPORTANTE: ouvir, capturar, interceptar, sniffar ou espionar redes às quais você não tem acesso legal é antiético e caracteriza crime.
Em redes sem fio ou com fio de transmissão é preciso configurar a captura na interface de rede em 'modo promíscuo' para conseguir capturar os pacotes que não são direcionados para a placa de rede do computador que está executando o Wireshark.

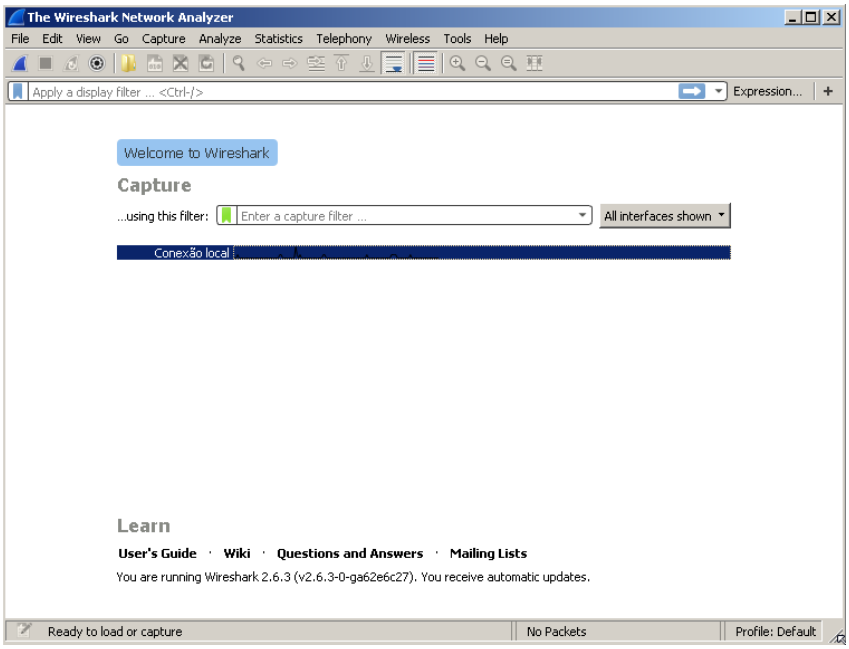
Orientações importantes antes de iniciar o seu trabalho:



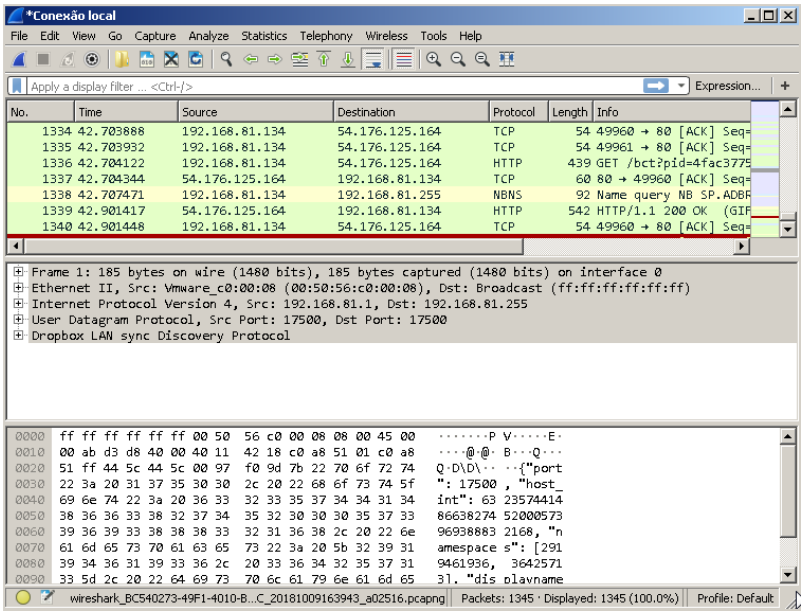
Orientações necessárias para instalar e compreender conceitos básicos sobre o uso do Wireshark. Após baixar, instalar e executar o Wireshark você deve fazer os seguintes passos:

1. Abrir o **Wireshark** (clicando no ícone do Desktop - caso tenha sido criado - ou através do menu de programas ou diretamente da pasta onde ele foi instalado

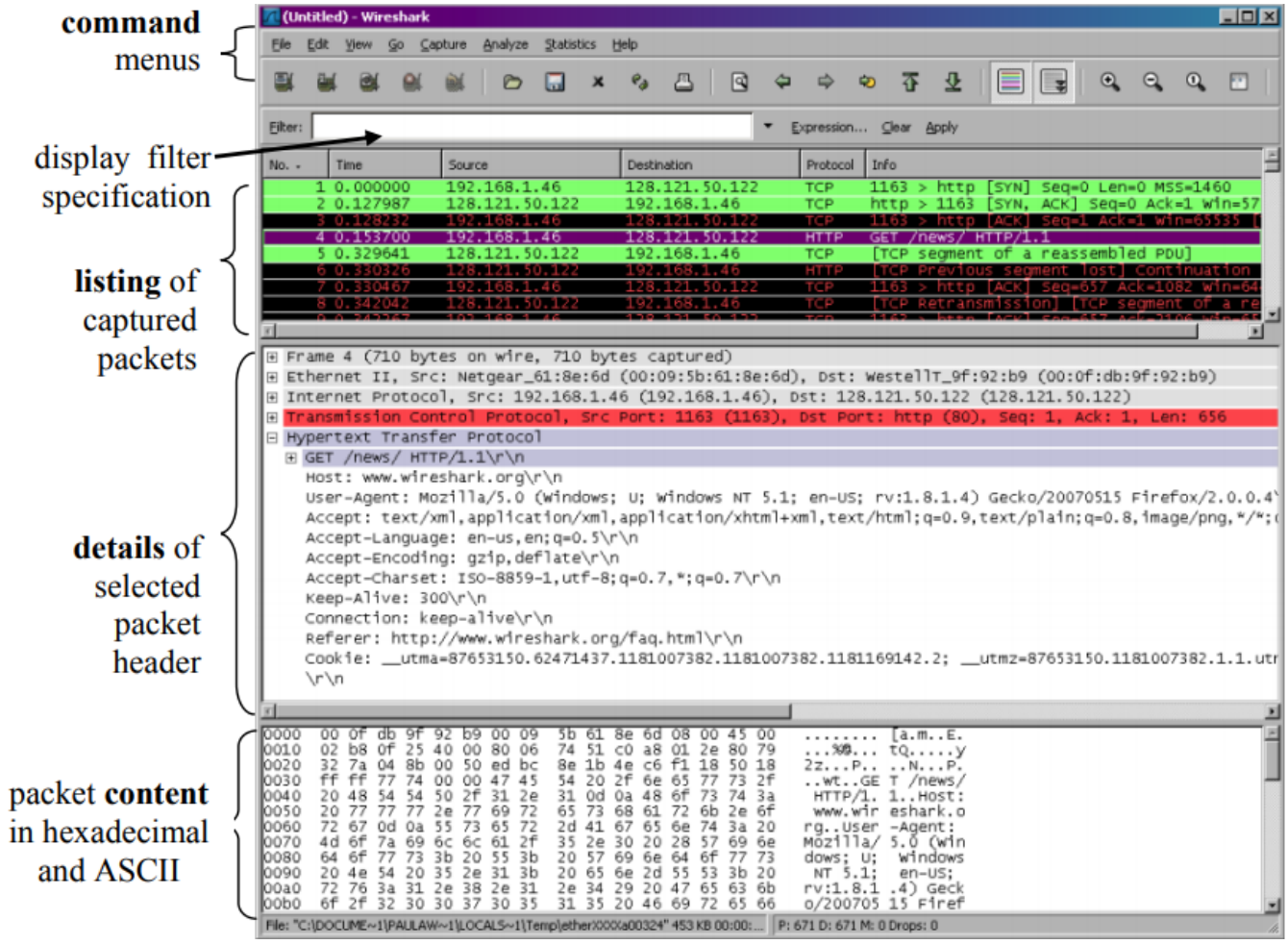
2. Será exibida a tela principal do Wireshark que é similar a tela a seguir. Pode ter pequenas diferenças dependendo da versão. O processo principal para iniciar o uso do Wireshark é a captura dos pacotes da rede. Você precisa identificar qual é a interface de rede utilizada. No caso da imagem abaixo, só existe uma interface cabeada no computador. No seu, também pode ser listada uma interface wireless por exemplo. Após escolhida a interface, basta dar "Enter" ou um duplo clique em cima do nome da interface de rede.



3. Se a instalação do Wireshark foi bem sucedida e sua placa de rede estiver funcionando corretamente, você deve rapidamente começar a ver linhas aparecendo na janela de captura de pacotes (veja exemplo abaixo). Cada linha representa um pacote (uma unidade de dados - em cada camada do modelo OSI ou da arquitetura TCP/IP o PDU - Protocol Data Unit - tem seu nome mais adequado (segmento, pacote/datagrama, quadro/frame), mas é genericamente chamado de pacote) que foi enviado através da rede e que o Wireshark detectou.
4. Mesmo que você não esteja solicitando ativamente qualquer informação (como pedir ao seu navegador para requisitar uma página web) o computador e os outros dispositivos da rede estão constantemente enviando mensagens entre si. Além disso, por si só, os programas no computador também podem estar enviando. informações através da rede (solicitações de atualização de software seria um exemplo). A tela a seguir mostra um exemplo de pacotes de rede que foram capturados pelo Wireshark.



5. As colunas diferentes da janela de exibição detalham o número e o tempo dos pacotes que foram capturados, a origem e destino para os pacotes, bem como o tipo de protocolo, comprimento e informações gerais sobre o pacote.
6. Você pode clicar duas vezes em um pacote para obter mais informações sobre ele.
7. A interface do Wireshark tem cinco componentes principais:



Os **menus de comando** são menus suspensos padrão, situados na parte superior da janela. O que nos interessa agora são os menus **"File"** e **"Capture"**. O menu File permite salvar dados em pacotes capturados ou abrir um arquivo contendo dados de pacotes capturados anteriormente, e sair do aplicativo Wireshark. O menu **"Capture"** permite que você comece a captura de pacotes.

A **janela de listagem de pacotes** exibe um resumo de uma linha para cada pacote capturado, incluindo o número do pacote (designado pelo Wireshark - isto não é um número de pacote contido no cabeçalho de algum protocolo), o momento em que o pacote foi capturado, endereços de origem e destino do pacote, o tipo de protocolo, e informações específicas do protocolo contido no pacote. A lista de pacotes pode ser classificada de acordo com qualquer uma dessas categorias, clicando sobre o nome da coluna. O campo tipo de protocolo lista o protocolo de mais alto nível que enviou ou recebeu este pacote, ou seja, o protocolo que é a fonte ou destino para este pacote.

A **janela de detalhes do cabeçalho do pacote** fornece detalhes sobre o pacote selecionado (destacado) na janela de listagem de pacotes. (Para selecionar um pacote na janela de listagem de pacotes, coloque o cursor sobre resumo de uma linha do pacote na janela de listagem de pacotes e clique com o botão esquerdo do mouse). Estes dados incluem informações sobre o quadro Ethernet (assumindo que o pacote foi enviado/recebido através de uma interface Ethernet) e de datagramas IP que contém esse pacote. A quantidade de detalhes Ethernet e da camada IP exibida pode ser expandida ou minimizada, clicando nas caixas menos (-) e mais (+) à esquerda da linha do quadro de Ethernet ou datagrama IP na janela de detalhes dos pacotes. Se o pacote foi transmitido através de TCP ou UDP, detalhes TCP ou UDP também serão exibidos, o que pode igualmente ser expandido ou minimizado.

Finalmente, os detalhes sobre o protocolo de mais alto nível que enviou ou recebeu este pacote também são fornecidos.

A **janela de conteúdo dos pacotes** exibe todo o conteúdo do quadro capturado, em ASCII e formato hexadecimal.

Na parte superior da interface gráfica do Wireshark, está o **campo de filtragem para exibição de pacotes**, em que um nome de protocolo ou outras informações podem ser inseridos de modo a filtrar as informações exibidas na janela de listagem de pacotes (e, portanto, as janelas do cabeçalho do pacote e do conteúdo dos pacotes). Na prática abaixo, vamos usar o campo de filtro de pacotes para o Wireshark esconder (não exibir) os pacotes, exceto aqueles que correspondem a mensagens HTTP, isto é, apenas mensagens HTTP serão exibidas.

A melhor maneira de aprender sobre qualquer tipo de software é experimentá-lo! Vamos supor que o seu computador está conectado à Internet através de uma interface Ethernet com fio. Na verdade, eu recomendo que você faça o primeiro teste com uma conexão cabeada.

Vamos agora utilizar o Wireshark para analisar o funcionamento do protocolo HTTP. Serão observados a interação pedido/resposta e os formatos das mensagens.

OBS: A atividade **não** deve ser respondida utilizando a navegação através de um servidor proxy intermediando as requisições, já que o proxy irá mascarar os endereços públicos do servidor Web.

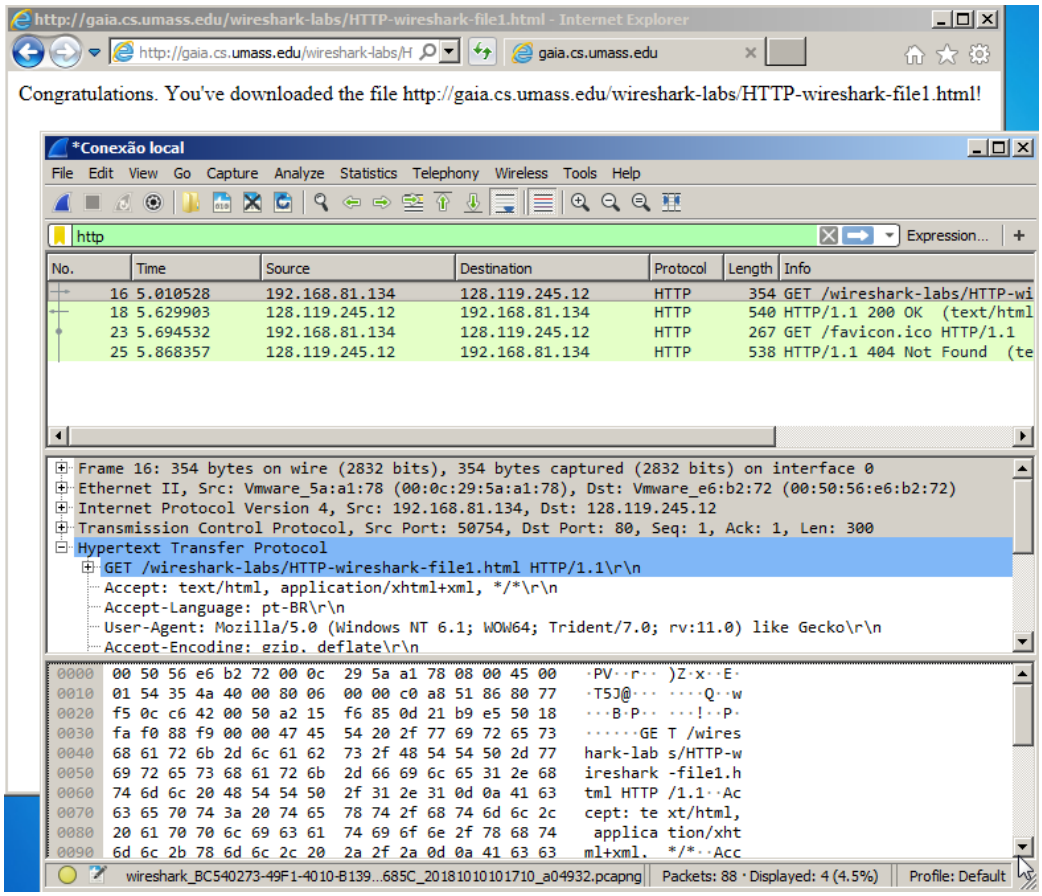
A partir desse ponto será apresentado o que você deve fazer no Wireshark para cumprir as atividades solicitadas.

PARTE 1 – Início da captura e análise do protocolo HTTP - Camada de Aplicação.

Interação HTTP requisição/resposta básica

(Fonte: Suplemento do Computer Networking: A Top-Down Approach, 7th ed., J.F. Kurose and K.W. Ross)

- Vamos fazer o acesso a um arquivo HTML que contém somente texto. Dessa forma, se trata de um arquivo que tem apenas um objeto;
- Feche todos os programas abertos no seu computador;
- Abra o Wireshark e acesse a tela de captura de pacotes, mas não inicie a captura ainda;
- Inicie o navegador (browser).
- Inicie a captura de pacotes no Wireshark.
- Acesse o endereço abaixo no seu Browser:
    - http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
- Seu navegador vai mostrar uma página web muito simples.
- Com os comandos ALT TAB ou utilize outra forma para retornar para o Wireshark;
- Pare a captura de pacotes (basta clicar no botão de Stop - quadradinho vermelho);
- Entre com '**http'** no filtro de pacotes, isso fará com que somente mensagens http sejam mostradas;
- Nesse momento você verá uma página bem parecida com a que está sendo mostrada na Figura a seguir
- Não se preocupe se aparecer mais pacotes, pois é comum ter outros serviços que foram acessados, mesmo que você não tenha acessado outras páginas. Lembre-se que podem ocorrer atualizações em segundo plano.



- O exemplo de captura mostrado na figura acima apresenta dois pacotes de mensagens HTTP (Pacotes 18 e 25) e duas mensagens do tipo GET (Pacotes 16 e 23);
- Lembre-se de que a mensagem HTTP é transportada em um segmento TCP, que é carregado em um datagrama IP, que é levado em um quadro Ethernet. O Wireshark exibe informações sobre o quadro ethernet, pacote IP, segmento TCP e protocolo de aplicação HTTP. Basta expandir clicando no "+" ao lado esquerdo dos protocolos.

Com base nas orientações fornecidas até aqui, analisando os pacotes das mensagens HTTP GET responda as seguintes questões:

Antes de iniciar a resposta das questões faça as seguintes apresentações/introduções:

- Iniciar o vídeo com a apresentação pessoal, informando seu nome completo, curso, disciplina, data, hora e a cidade em que mora.
- Comentar ou ler a último texto (Tweet) postado no twiter do professor que está disponível no endereço: http://twitter.com/teixeira_sergio; (Para caracterizar que o vídeo é atual) Não precisa ter conta no twitter ou seguir o professor. Esse link é público. Basta acessar o link para ter acesso ao último post.
- Com base nas orientações apresentadas e após a análise dos pacotes capturados, responda de forma consistente e fundamentada as questões abaixo e as demais questões indicadas nas outras partes.

Questão 1.1. O seu navegador executa a versão 1.0 ou 1.1 do HTTP? Qual a versão do HTTP que está rodando no servidor?

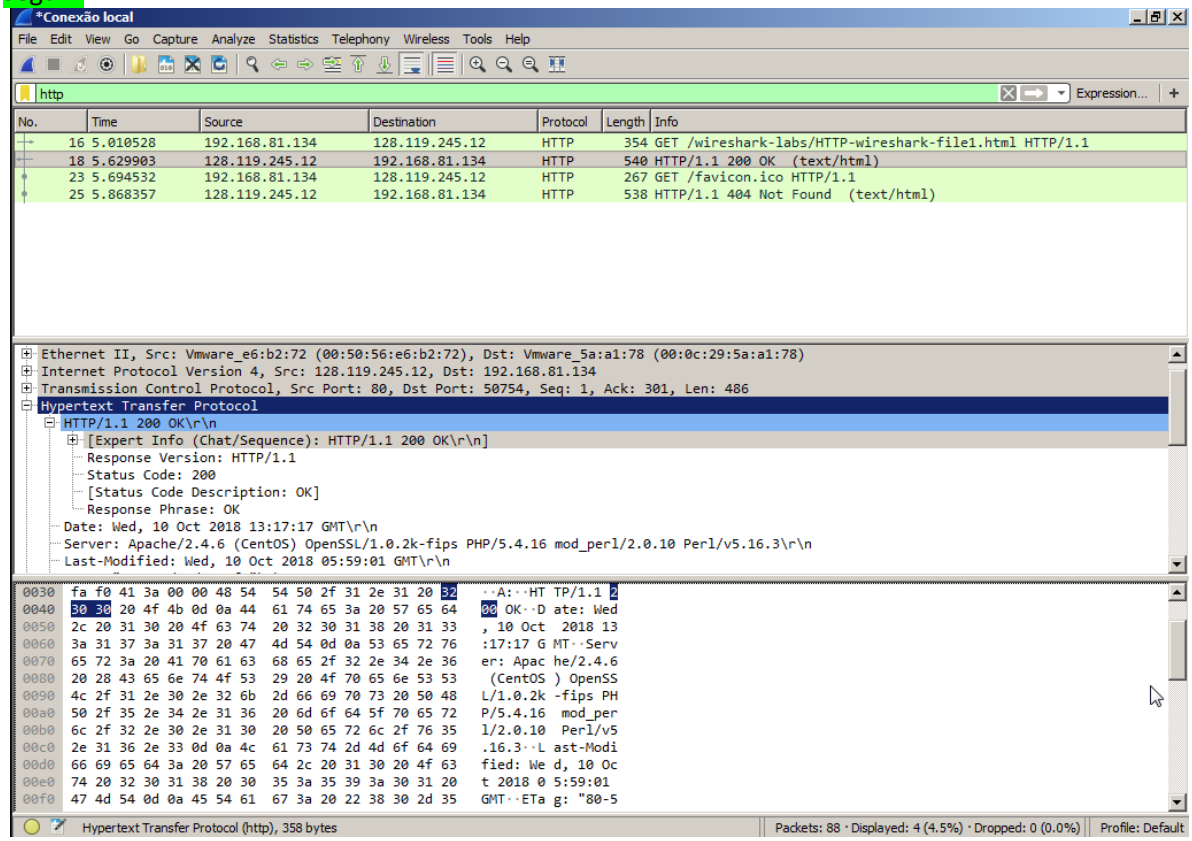
Questão 1.2. Quais linguagens (idiomas) o seu navegador indica que pode aceitar do servidor?

Questão 1.3. Qual o endereço IP do seu computador? E do servidor gaia.cs.umass.edu?

Questão 1.4. Qual aplicação (e versão) é utilizada pelo servidor web gaia.cs.umass.edu?

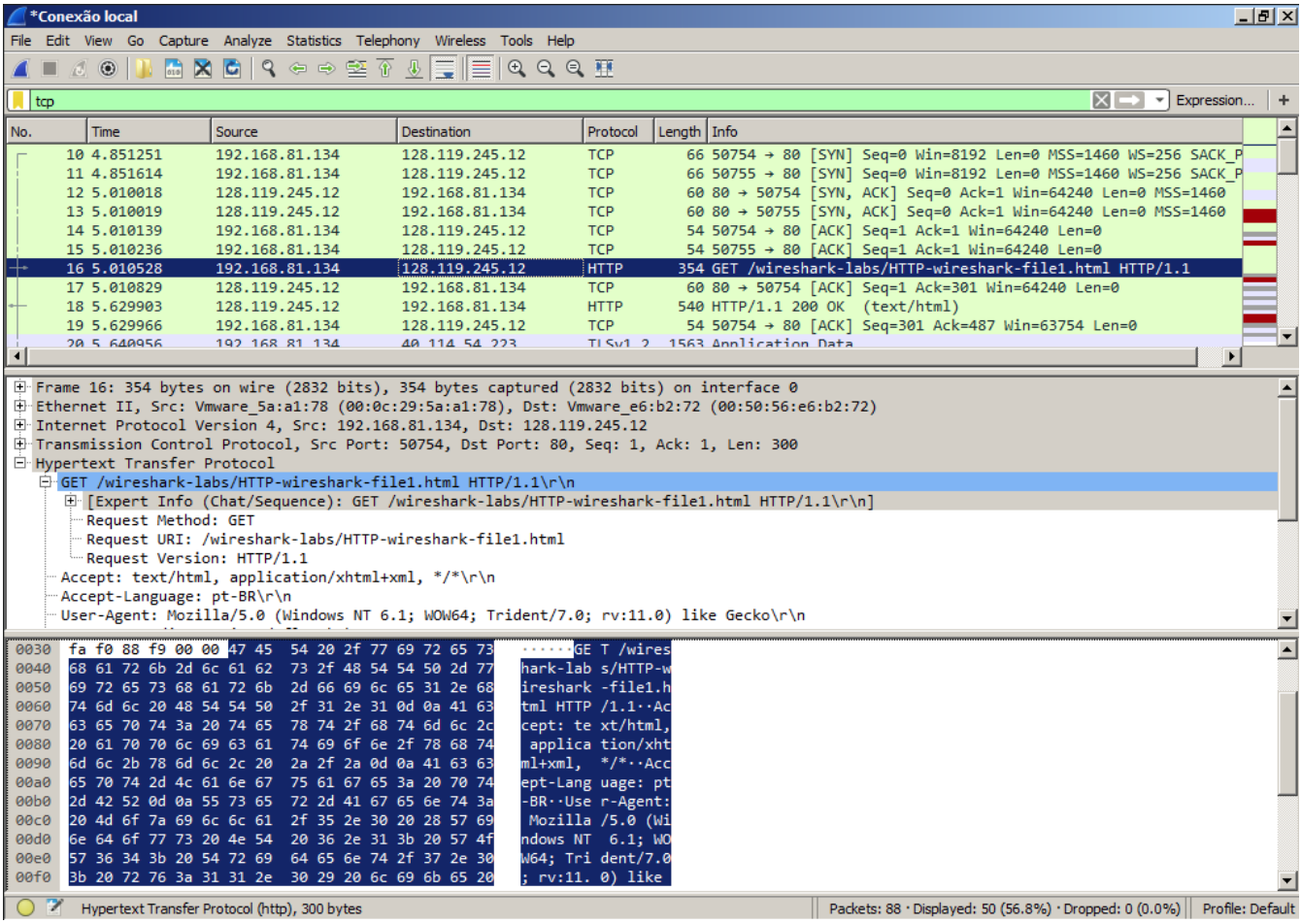
As questões 1.1, 1.2 e 1.3 podem ser respondidas com informações que estão na mesma captura da imagem mostrada previamente

Para a resposta da questão 1.4, basta selecionar o fluxo de resposta do servidor web conforme indica a tela a seguir:



PARTE 2 – Captura e análise do protocolo TCP - Camada de Transporte.

- Agora, vamos analisar o comportamento da conexão TCP em detalhes.
- Primeiro, filtre os pacotes exibidos na janela do Wireshark digitando “tcp” (em minúsculas, sem aspas e pressionando Enter) no campo de filtro de pacotes (utilizando a mesma captura anterior - basta digitar tcp no lugar de http).
- O que você deve ver é uma série de mensagens TCP e HTTP entre o seu computador e o host gaia que você acessou previamente `gaia.cs.umass.edu`. Você deve ver o handshake triplo inicial contendo uma mensagem SYN. Você também deve ver segmentos TCP ACK sendo retornados de gaia.cs.umass.edu para o seu computador. Além disso, verá também uma mensagem HTTP GET (utilizada na parte 1 anterior).



Observando as informações do fluxo TCP, responda às seguintes questões:

Questão 2.1. Qual é o número da porta TCP usada pelo seu computador cliente (source) para requisitar o arquivo html para gaia.cs.umass.edu? E qual o número de porta TCP que o servidor gaia está usando para receber e enviar essas respostas?

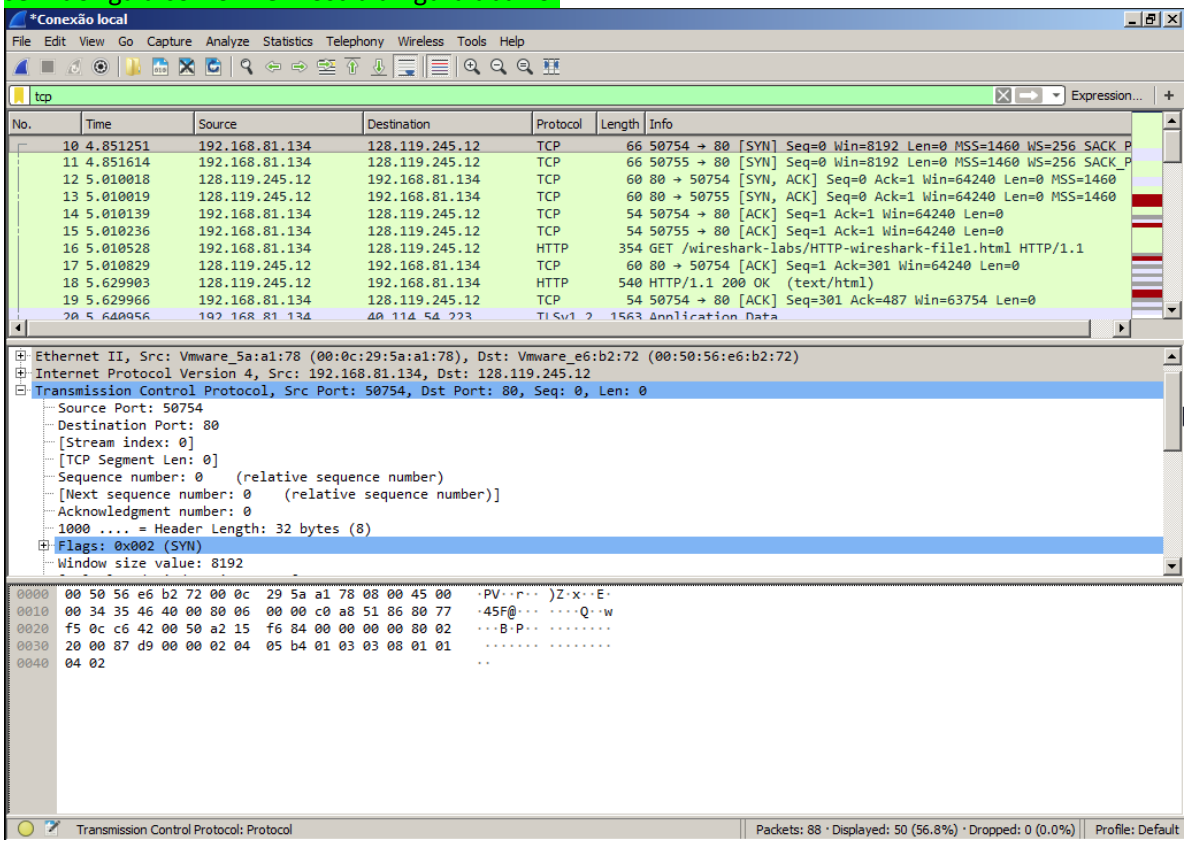
Questão 2.2. Mostre e comente o pacote que contém o segmento TCP SYN que caracteriza o início de uma conexão TCP (estabelecimento inicial de conexão - three way handshake) entre o computador cliente e o gaia.cs.umass.edu?

Questão 2.3. Após responder à questão 2.2 mostre e comente o campo do segmento TCP que contém o tamanho da janela utilizada pelo TCP para o controle de fluxo? Qual é o tamanho da janela em bytes?

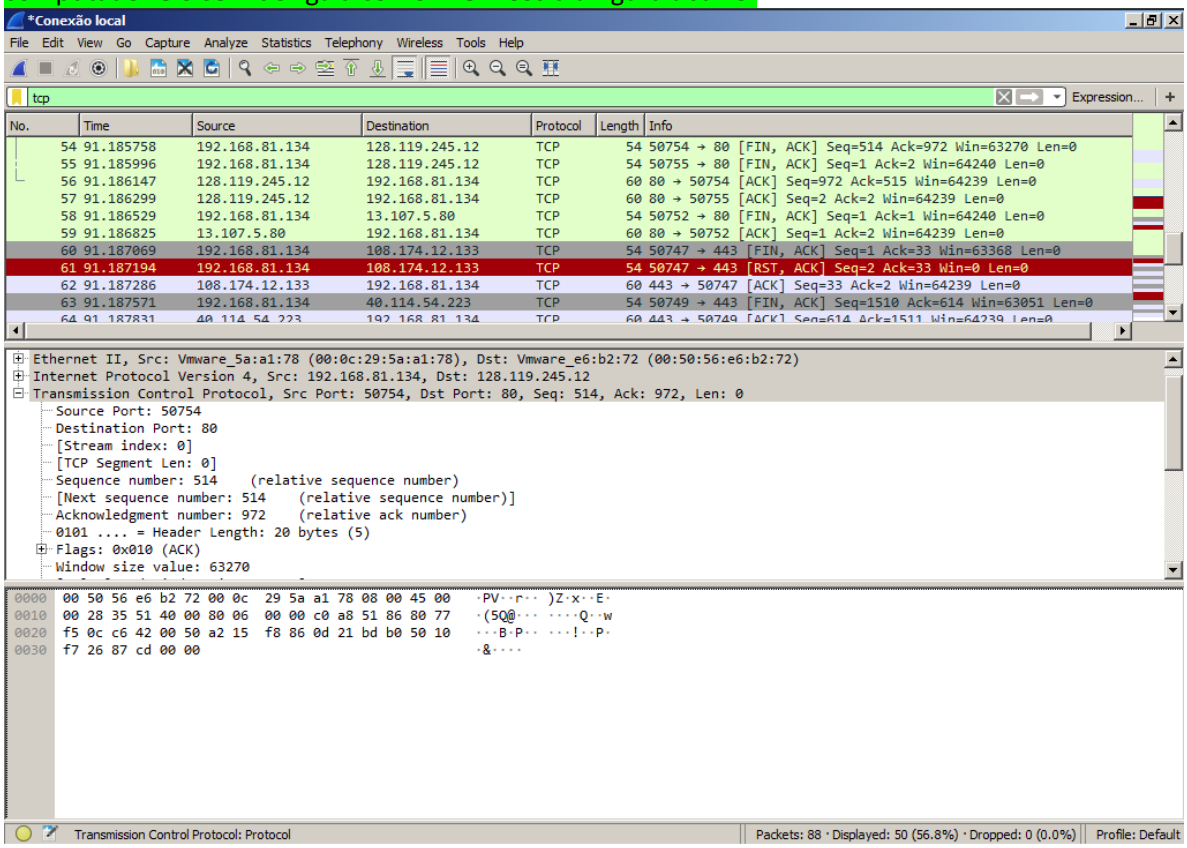
Questão 2.4. Identifique, abra e mostre o pacote do segmento TCP responsável pelo término da conexão. Qual é a flag que o TCP usa para encerrar a conexão? Mostre e diga qual é essa flag.

As questões 2.1 e 2.2 podem ser respondidas com informações que estão na mesma captura da imagem mostrada previamente.

Para responder a questão 2.3 você precisa identificar o pacote que tem o segmento TCP SYN de conexão com o servidor gaia conforme mostra a figura abaixo:



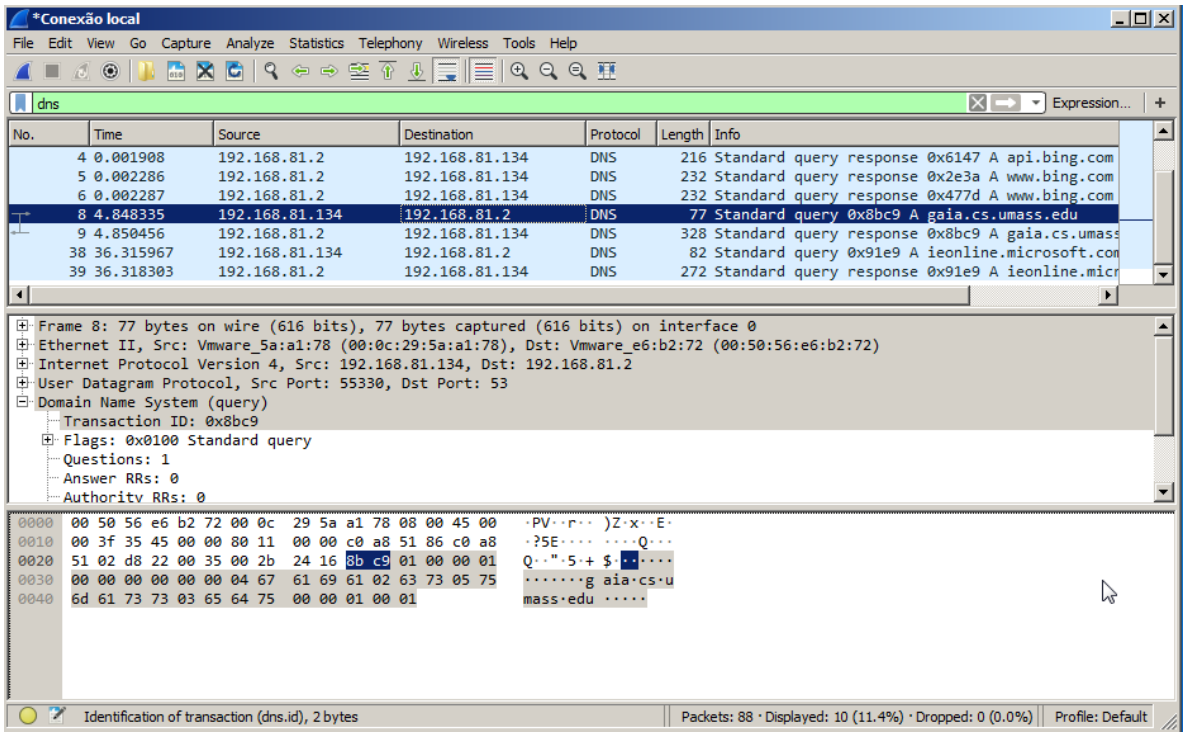
Para a resposta da questão 2.4 basta selecionar o fluxo que contém o segmento de finalização da conexão entre o computador e o servidor gaia conforme mostra a figura abaixo:



PARTE 3 – Captura e análise do protocolo DNS - Camada de Aplicação.

- O Sistema de Nomes de Domínio (DNS) traduz domínios (hostnames) para endereços IP, cumprindo um papel crítico na infraestrutura da Internet. Nessa prática, vamos dar uma olhada no lado do cliente DNS. Lembre-se de que o papel do cliente no DNS é relativamente simples - um cliente (seu computador, por exemplo) envia uma consulta ao seu servidor DNS local e recebe uma resposta de volta. Mas muita coisa do que é feito fica "invisível", transparente para os clientes DNS, como hierarquicamente os servidores DNS (root servers, top-level domains, etc) comunicam-se entre si para resolver de forma recursiva ou iterativa a consulta DNS do cliente.
- Nesta prática, iremos observar a consulta ao domínio gaia.cs.umass.edu e a resposta do servidor DNS, que informará o endereço IP através de uma mensagem DNS de resposta.
- Com o fluxo ainda da prática da parte 1, filtre os fluxos DNS simplesmente digitando dns no campo de filtragem do Wireshark. Sua tela deverá ficar semelhante a da imagem abaixo.
- Caso o seu fluxo não exiba corretamente essa requisição e resposta, será necessário limpar o cache DNS do seu computador. Se você não conseguiu identificar esses pacotes será necessário limpar o cache do DNS no seu computador.
- Para limpar o cache DNS do seu computador, basta utilizar o comando no prompt do windows: **ipconfig /flushdns**
- Após limpar o cache do DNS é preciso refazer a captura conforme orientações apresentadas previamente no início desse trabalho.

(ATENÇÃO, só faça esse procedimento de limpeza do cache e repetição da captura se você não identificar pacotes conforme é mostrado na figura abaixo)



Observando as informações da consulta e resposta DNS, responda às seguintes questões:

Questão 3.1. Identifique e comente a mensagem de consulta ao DNS para descobrir o IP do host 'gaia.cs.umass.edu'. Qual foi o protocolo da camada de transporte utilizado?

Questão 3.2. Após responder à questão 3.1 identifique e comente a porta destino usada para a consulta DNS?

Questão 3.3. Qual é o endereço IP do servidor de DNS que foi usado para a resolução do endereço IP do host 'gaia.cs.umass.edu'?

Para responder as questões acima você deve identificar uma tela similar ao que foi mostrado na imagem mostrada previamente.

PARTE 4 – Captura e análise do protocolo Ethernet - Camada de Enlace.

- O Endereço MAC (Media Access Control) é um endereço físico associado às interfaces de rede. É um endereço único, e é utilizado para controle de acesso em redes de computadores.
- Agora, vamos analisar os endereços MAC (origem e destino) envolvidos nas questões abaixo.
- Para verificar os endereços envolvidos, basta expandir (botão + à esquerda do protocolo) o Ethernet II na janela de detalhes do pacote selecionado.

Questão 4.1. Após responder à questão 3.3, identifique e comente sobre o endereço MAC do seu computador?

Questão 4.2. Qual é o endereço MAC do host `gaia.cs.umass.edu`? Justifique e fundamente a sua resposta.

A questão 4.1 pode ser respondida com informações que estão na mesma captura da imagem da parte 3 mais acima.

Um grande abraço e sucesso no trabalho,
Sérgio Teixeira e
José Gonçalves Pereira Filho.

CRITÉRIOS DE CORREÇÃO DO TRABALHO			
Item	**Descrição**	**Critério de avaliação**	**Pontuação**
Parte 1	**Questão 1.1.**	Demonstrou que tem domínio técnico do assunto abordado? Respondeu à questão corretamente?	
	Questão 1.2.	Demonstrou que tem domínio técnico do assunto abordado? Respondeu à questão corretamente?	
	Questão 1.3.	Demonstrou que tem domínio técnico do assunto abordado? Respondeu à questão corretamente?	
	Questão 1.4.	Demonstrou que tem domínio técnico do assunto abordado? Respondeu à questão corretamente?	
Parte 2	**Questão 2.1.**	Demonstrou que tem domínio técnico do assunto abordado? Respondeu à questão corretamente?	
	Questão 2.2.	Demonstrou que tem domínio técnico do assunto abordado? Respondeu à questão corretamente?	
	Questão 2.3.	Demonstrou que tem domínio técnico do assunto abordado? Respondeu à questão corretamente?	
	Questão 2.4.	Demonstrou que tem domínio técnico do assunto abordado? Respondeu à questão corretamente?	
Parte 3	**Questão 3.1.**	Demonstrou que tem domínio técnico do assunto abordado? Respondeu à questão corretamente?	
	Questão 3.2.	Demonstrou que tem domínio técnico do assunto abordado? Respondeu à questão corretamente?	
	Questão 3.3.	Demonstrou que tem domínio técnico do assunto abordado? Respondeu à questão corretamente?	
Parte 4	**Questão 4.1.**	Demonstrou que tem domínio técnico do assunto abordado? Respondeu à questão corretamente?	
	Questão 4.2.	Demonstrou que tem domínio técnico do assunto abordado? Respondeu à questão corretamente?	
		Pontuação →	