Guia 1 – Wireshark[1]

Objectivos:

- Introdução à captura e análise de pacotes
- Introdução ao wireshark

Primeiro contacto

1. Inicie o *browser*, que exibirá a página inicial selecionada. Inicie o software Wireshark. Verá inicialmente uma janela que espera que identifique o interface de captura - o Wireshark ainda não começou a capturar pacotes.

2. Para iniciar a captura de pacotes, selecione a opção "Iniciar", ou no menu Capturar e selecione Interfaces. Isso fará com que a janela "Wireshark: Capture Interfaces" seja exibida e aí deverá ver uma lista de interfaces, onde deverá selecionar um através da opção "Capturar".

3. Com o wireshark a capturar pacotes, use o browser para aceder ao URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html.

4. Para exibir esta página, o browser entrará em contato com o servidor HTTP em gaia.cs.umass.edu e trocará mensagens HTTP com o servidor para fazer o download desta página. Os pacotes Ethernet ou WiFi contendo essas mensagens HTTP (assim como todos os outros pacotes que passam pelo seu adaptador Ethernet ou WiFi) serão capturados pelo Wireshark.

5. Depois de o browser exibir a página INTRO-wireshark-file1.html (é uma simples linha de parabéns), interrompa a captura de pacotes do Wireshark selecionando parar na janela de captura do Wireshark.

O wireshark mostra dados dos pacotes ativos que contêm todas as mensagens de protocolo trocadas entre o computador e outras entidades de rede! As trocas de mensagens HTTP com o servidor web gaia.cs.umass.edu devem aparecer em algum lugar na lista de pacotes capturados. Mas há muitos outros tipos de pacotes exibidos também. Veja, por exemplo, os diversos tipos de protocolo mostrados na coluna Protocolo. Mesmo que a única ação que você tenha feito tenha sido baixar uma página da web, evidentemente havia muitos outros protocolos em execução em seu computador que não eram vistos pelo utilizador. Aprenderá muito mais sobre esses protocolos na UC de

[1] *- Retirado de "Wireshark Lab: Getting Started v8.1 - Supplement to Computer Networking: A Top-Down Approach, 8th ed., J.F. Kurose and K.W. Ross"*

Fundamentos de redes de computadores! Por enquanto, fique ciente de que normalmente há muito mais a acontecer do que vemos. E por vezes coisas indesejáveis.

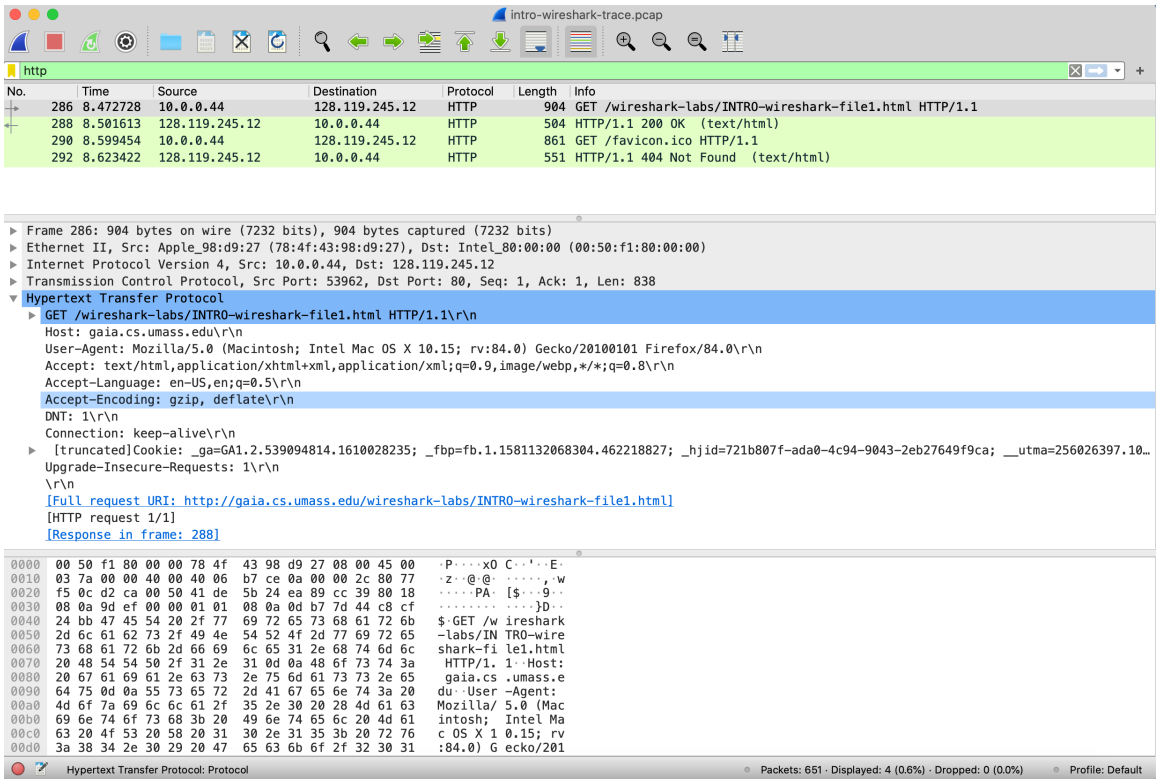
6. Inspecione o conteúdo da primeira solicitação HTTP GET do seu browser para o servidor. Consegue ver uma linha "IF-MODIFIED-SINCE" no HTTP GET?

7. Normalmente os pacotes capturados são tantos que se torna difícil encontrar o que queremos. Uma das formas de evitar isso é, e quando pudemos, é sermos rápidos a provocar a experiência e parar rapidamente o processo de captura.

8. Digite "http" (sem as aspas e em minúsculas – todos os nomes de protocolos estão em minúsculas no Wireshark e certifique-se de pressionar a tecla Enter/Return) na janela de especificação do filtro de exibição na parte superior da tela principal Janela do Wireshark. Em seguida, selecione Aplicar (à direita de onde você digitou "http") ou apenas pressione retornar. Isso fará com que apenas a mensagem HTTP seja exibida na janela de listagem de pacotes.

9. Observe também que na janela Detalhes do pacote selecionado, optamos por mostrar o conteúdo detalhado da mensagem do aplicativo Hypertext Transfer Protocol que foi encontrada no segmento TCP, que estava dentro do datagrama IPv4 que estava dentro do quadro Ethernet II (WiFi). Concentrar-se no conteúdo de uma mensagem, segmento, datagrama e nível de quadro específico nos permite focar apenas no que queremos ver[2].

[2] Conteúdo de uma mensagem, segmento, datagrama e nível de quadro são nomes que os pacotes assumem em cada camada da pilha protocolar. Por comodidade usamos pacote e indicamos a camada.



10. Encontre a mensagem HTTP GET que foi enviada do seu computador para o servidor HTTP gaia.cs.umass.edu. (Procure uma mensagem HTTP GET na parte "listing of captured packets" da janela do Wireshark que mostra "GET" seguido pela URL gaia.cs.umass.edu que você digitou. A mensagem HTTP GET, o quadro Ethernet, o datagrama IP, o segmento TCP e as informações do cabeçalho da mensagem HTTP serão exibidos na janela de cabeçalho do pacote. Ao clicar nas setas apontando alternadamente para a direita e para baixo.

11. No lado esquerdo da janela de detalhes do pacote, minimize a quantidade de informações de Frame, Ethernet, Internet Protocol e Transmission Control Protocol exibida. (Observe, em particular, a quantidade minimizada de informações de protocolo para todos os protocolos, exceto HTTP, e a quantidade maximizada de informações de protocolo para HTTP na janela de cabeçalho do pacote).

12. Responda agora às seguintes questões:

- Identifique os protocolos que aparecem na sua captura: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2.

- Quanto tempo levou desde o envio da mensagem HTTP GET até o recebimento da resposta HTTP OK? (Por defeito, o valor da coluna Time na janela de listagem de pacotes é a quantidade de tempo, em segundos, desde que o rastreamento do Wireshark começou.

- Qual é o endereço de Internet do gaia.cs.umass.edu (também conhecido como www-net.cs.umass.edu)? Qual é o endereço de Internet do seu computador?

- Interrompa a captura de pacotes do Wireshark e digite “http” na janela de especificação do filtro de exibição, de forma que apenas as mensagens HTTP capturadas sejam exibidas posteriormente na janela de listagem de pacotes.

- Expanda as informações sobre a mensagem HTTP na janela Wireshark “Detalhes do pacote selecionado”) para que você possa ver os campos na mensagem do pedido HTTP GET. Que tipo de navegador da Web emitiu a solicitação HTTP? A resposta é mostrada na extremidade direita das informações após o campo “User-Agent:” da mensagem HTTP expandida. Este valor de campo na mensagem HTTP é como um servidor da web aprende que tipo de navegador você está a usar (e.g. Firefox, Safari, Microsoft Internet Edge)
- Utilizando a opção conversations do menu Statistics, identifique os pares de estações que mais comunicam.
- Utilizando a opção protocol hierarchy do menu Statistics, identifique os pacotes com maior utilização na captura realizada.

13. Submeta as respostas na plataforma de e-learning.