Lista de Exercícios - WireShark - Redes de Computadores
Júlio Melo Campos - 22250349

Seção 2.1

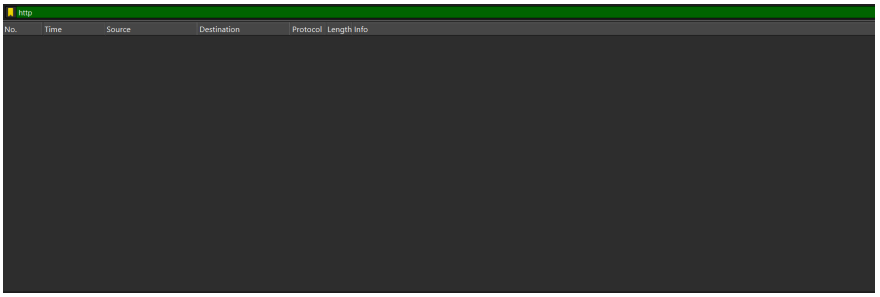
1- Quais dos seguintes protocolos são mostrados como aparecendo (ou seja, estão listados na coluna "protocolo" do Wireshark) em seu arquivo de rastreamento: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2?

R: Estão listados protocolos como: QUIC, TCP, ARP, DNS e TLS v1.2.

4178	2024-10-06 1…	192.168.15.8	34.128.128.0	TLSv1.2
4179	2024-10-06 1…	192.168.15.8	34.128.128.0	TCP
4180	2024-10-06 1…	192.168.15.8	34.128.128.0	TLSv1.2
4181	2024-10-06 1…	192.168.15.8	34.128.128.0	TCP
4182	2024-10-06 1…	192.168.15.8	192.168.15.1	DNS
4183	2024-10-06 1…	192.168.15.8	192.168.15.1	DNS
4184	2024-10-06 1…	142.250.219.1	192.168.15.8	TCP
4185	2024-10-06 1…	142.251.132.228	192.168.15.8	QUIC
4186	2024-10-06 1…	fe80::c23d:d9ff:feb…	fe80::d196:2d6a:1fa…	DNS
4187	2024-10-06 1…	192.168.15.1	192.168.15.8	DNS
4188	2024-10-06 1…	192.168.15.8	15.204.182.92	TCP
4189	2024-10-06 1…	192.168.15.8	15.204.182.92	TCP
4190	2024-10-06 1…	34.128.128.0	192.168.15.8	TCP
4191	2024-10-06 1…	34.128.128.0	192.168.15.8	TLSv1.2
4192	2024-10-06 1…	142.251.132.228	192.168.15.8	QUIC
4193	2024-10-06 1…	34.128.128.0	192.168.15.8	QUIC
4194	2024-10-06 1…	34.128.128.0	192.168.15.8	QUIC
4195	2024-10-06 1…	142.251.129.3	192.168.15.8	QUIC
4196	2024-10-06 1…	192.168.15.8	142.251.129.3	QUIC
4197	2024-10-06 1…	192.168.15.8	142.251.129.3	QUIC
4198	2024-10-06 1…	142.251.129.3	192.168.15.8	QUIC
4199	2024-10-06 1…	192.168.15.8	142.251.132.228	QUIC
4200	2024-10-06 1…	192.168.15.8	142.251.132.228	QUIC
4201	2024-10-06 1…	142.251.132.228	192.168.15.8	QUIC
4202	2024-10-06 1…	142.251.132.228	192.168.15.8	QUIC
4203	2024-10-06 1…	192.168.15.8	142.251.132.228	QUIC

2- Faça o exercicio 2 e 3 utilizando 1o o endereço https://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html e depois o endereço http://httpforever.com , tanto em casa como na universidade. Quanto tempo demorou desde o envio da mensagem HTTP GET até o recebimento da resposta HTTP OK? (Por padrão, o valor da coluna Time na janela de listagem de pacotes é a quantidade de tempo, em segundos, desde o início do rastreamento do Wireshark. (Se você deseja exibir o campo Time no formato de hora do dia, selecione o botão Wireshark Visualize o menu suspenso, selecione Formato de exibição de hora e selecione Hora do dia .)

R: No meu computador, não houve aparecimento dos pacotes lançados pelos links acima pela rede Wi-Fi.



Porém, o tempo médio entre o envio da mensagem HTTP GET até o recebimento da resposta HTTP OK, leva em torno de 500 ms. Levando em consideração, os parâmetros abaixo:

$$150ms(handshake) + 150ms(GET) + 50ms(processamento) + 150ms(resposta) = 500ms$$

Para conexões locais, a média pode ser bem rápida, abaixo de 200 ms, enquanto para conexões internacionais, pode ultrapassar 500 ms, dependendo das condições da rede e do servidor.

3 - Pesquise sobre o que são o http e https e responda porque na universidade não foi possível visualizar as mensagens HTTP do endereço http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html (ex. GET e response na universidade)

R: HTTP é o protocolo padrão para transferência de dados nas web, são transmitidos em textos simples, podendo ser visto por todos que interceptam os pacotes de dados, operando na porta 80 por padrão, por outro lado, o HTTPS é uma versão secura do http com os dados transmitidos repassados por meio de uma camada de criptografia (SSL/TLS), garantindo confidencialidade de dados, e autenticação de identidade dos servidores, operando na porta 443 por padrão. Ele é extremamente protegido contra ataques de man-in-the-middle.

E provavelmente a rede da universidade e o firewall bloqueia ou força o uso de HTTPS para proteger a comunicação, e como o Wireshark não consegue decodificar tráfego criptografado sem as chaves de criptografia, não é possível ver as mensagens HTTP (Get e Response).

4 - Qual é o endereço de Internet de www-net.cs.umass.edu e de httpforever.com? Qual é o endereço de Internet do seu computador ou (se você estiver usando o arquivo de rastreamento) do computador que enviou a mensagem HTTP GET?

R: O endereço IP do site www-net.cs.umass.edu é 128.119.245.12. Para o site httpforever.com, no entanto, não foi possível identificar um IP válido atualmente, o que pode indicar que o domínio não está em uso ativo ou está desatualizado. Visto que é dado como não seguro ao acessá-lo. Usando o wireshark, é possível identificar o endereço de Internet do computador que é 177.207.112.206.

5 - Expanda as informações sobre a mensagem HTTP na janela "Detalhes do pacote selecionado" do Wireshark para que você possa ver os campos na mensagem de solicitação 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:" na exibição de mensagem HTTP expandida. [Esse valor de campo na mensagem HTTP é como um servidor da Web descobre que tipo de navegador você está usando.]

R: Baseado no navegador que foi utilizado ao pesquisar o link, podem ser entre Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, e outros, geralmente são responsáveis por

emitir solicitações HTTP quando você acessa um site. No caso, poderia ser o Google Chrome pelo fato de ser o utilizado no momento da pesquisa.

6 - Expanda as informações sobre o Protocolo de Controle de Transmissão para este pacote na janela "Detalhes do pacote selecionado" do Wireshark (consulte a Figura 3 na redação do laboratório) para que você possa ver os campos no segmento TCP que transporta a mensagem HTTP. Qual é o número da porta de destino (o número após "Dest Port:" para o segmento TCP que contém a solicitação HTTP) para a qual esta solicitação HTTP está sendo enviada?

R: O número da porta de destino para uma solicitação HTTP é normalmente 80 para HTTP e 443 para HTTPS. Isso ocorre porque os servidores web padrão escutam essas portas para receber solicitações de navegadores ou outros clientes web. Pode ser observado abaixo de um protocolo do tipo TCP.