Nome: Yuri Lanzini Matrícula: 2221100006

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

Questão 1.1: O seu navegador executa a versão 1.0 ou 1.1 do HTTP? Qual a versão do HTTP que está rodando nos servidores da UFFS e da RNP?

R:

O navegador e o servidor da UFFS estão utilizando a versão 1.1 do HTTP.
O servidor da RNP está utilizando a versão 2.0 do HTTP.

Questão 1.2: Quais linguagens (idiomas) o seu navegador indica que pode aceitar dos servidores?

R:

O navegador indica que pode aceitar os seguintes idiomas dos servidores:

- pt-BR (Português do Brasil)
- pt (Português)
- en-US (Inglês dos Estados Unidos)
- en (Inglês geral)

Questão 1.3: Qual o endereço IP do seu computador? E dos servidores da UFFS e da RNP?

R:

Endereços IP capturados pelo Wireshark, são:

- IP do meu computador: 192.168.1.103
- IP da UFFS: 200.135.49.107
- IP da RNP: 104.18.26.22

Questão 1.4: Qual aplicação (e versão) é utilizada pelos servidores web da UFFS e da RNP?

R:

O servidor da UFFS está utilizando Zope/(2.13.24, python 2.7.6, linux2) ZServer/1.1.
O servidor da RNP está utilizando o Cloudflare.

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

Questão 2.1: Qual é o número da porta TCP usada pelo seu computador cliente (source) para requisitar as páginas da UFFS e da RNP? E qual o número de porta TCP que os servidores da UFFS e da RNP estão usando para receber e enviar essas respostas?

R:

O número da porta TCP usada pelo computador cliente (source) para requisitar páginas da UFFS: 44652

O número da porta TCP usada pelo computador cliente (source) para requisitar páginas da RNP: 56024

O número de porta TCP dos servidores da UFFS e da RNP: 443

Questão 2.2: Mostre e comente o pacote que contém o segmento TCP SYN que caracteriza o início de uma conexão TCP entre o computador cliente e os servidores da UFFS e RNP.

R:

UFFS:

Source	Destination	Protocol	Length	Info
192.168.1.103	200.135.49.107	TCP	74	44652 → 443 [SYN]

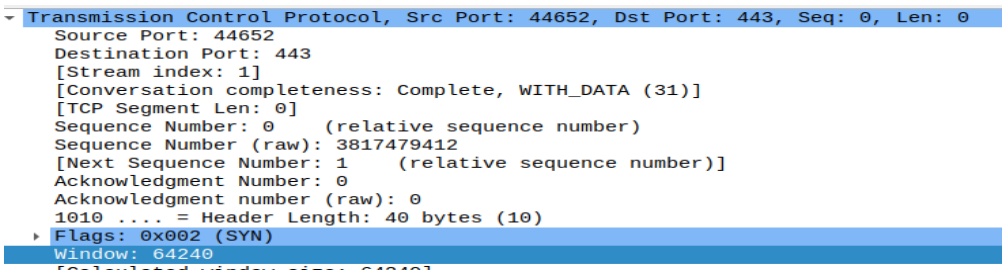
RNP:

Source	Destination	Protocol	Length	Info
192.168.1.103	104.18.26.22	TCP	74	56024 → 443 [SYN]

Este pacote SYN inicia a comunicação TCP entre meu computador e o servidor da RNP, estabelecendo o número de sequência inicial, as opções de controle de fluxo, e o tamanho da janela. O destino é a porta 443, confirmando que o tráfego é criptografado via HTTPS. As opções TCP indicam suporte para características avançadas como SACK e window scaling, otimizando o controle de congestionamento e a eficiência da conexão.

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?

R:

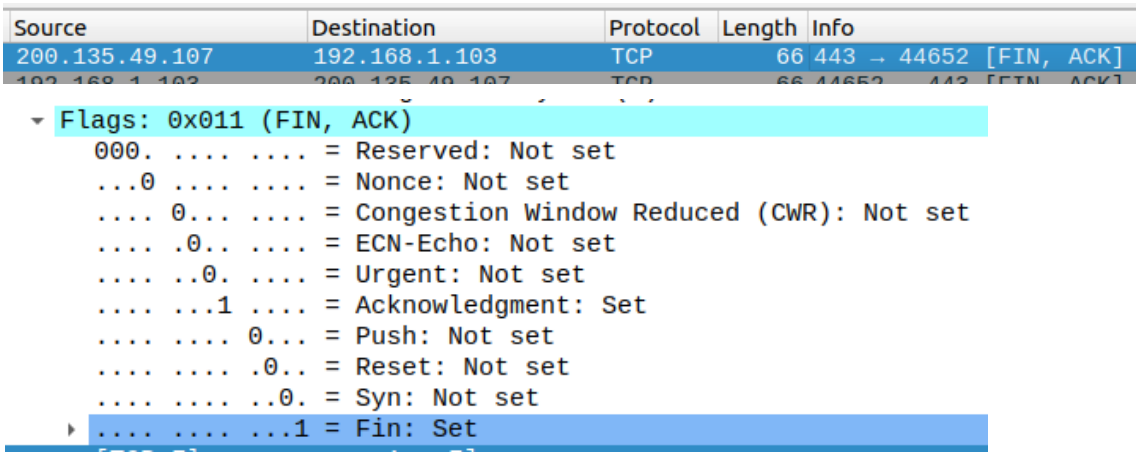


Nos pacotes analisados dos servidores da UFFS e da RNP, o campo Window (tamanho da janela) tem o valor de 64240 bytes. Este valor indica a capacidade de recepção do cliente, ou seja, a quantidade de dados que o cliente pode receber sem precisar enviar uma confirmação (ACK).

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 explique qual é essa flag.

R:

A flag que o TCP usa para encerrar a conexão é a FIN (Finish): Esta flag é ativada quando o remetente deseja encerrar a conexão TCP. Ao definir a flag FIN, o remetente está informando ao receptor que não tem mais dados para enviar.



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

Questão 3.1: Identifique e comente a mensagem de consulta ao DNS para descobrir o IP dos hosts da UFFS e RNP. Qual foi o protocolo da camada de transporte utilizado?

R:

A consulta DNS é enviada para o servidor DNS localizado no endereço IP (192.168.1.1). Tem como objetivo descobrir informações sobre o domínio www.uffs.edu.br e www.rnp.br, especificamente para o tipo de serviço HTTPS. A consulta é feita usando o protocolo UDP, que é o protocolo padrão para consultas DNS devido à sua natureza leve e rápida.

Questão 3.2: Qual é a porta destino usada para a consulta DNS?

R:

A porta destinada para consulta DNS da UFFS e RNP é a 53.

Questão 3.3: Qual é o endereço IP do servidor de DNS que foi usado para a resolução do endereço IP dos hosts da UFFS e RNP?

R:

O servidor DNS que meu computador utilizou para resolver os endereços IP dos hosts da UFFS e da RNP foi o 192.168.1.1, que é o endereço do meu roteador local. No entanto, os endereços IP reais dos servidores da UFFS e RNP, conforme capturados pelo Wireshark, são:

- UFFS: 200.135.49.107
- RNP: 104.18.26.22

O roteador atua como intermediário entre o meu computador e a internet, encaminhando as consultas DNS para servidores DNS externos e retornando as respostas ao meu computador.

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

Questão 4.1: Identifique e comente sobre o endereço MAC do seu computador.

R:

O endereço MAC do meu computador, conforme identificado no pacote, é 34:c9:3d:f4:27:2f. Esse endereço é um identificador único atribuído à interface de rede do meu computador. Endereços MAC são usados para garantir que os pacotes de dados sejam entregues corretamente dentro da rede local, fornecendo um meio de identificação de dispositivos.

Questão 4.2: Qual é o endereço MAC dos servidores da UFFS e RNP? Justifique e fundamente a sua resposta.

R:

O endereço MAC que aparece para os servidores da UFFS e da RNP é na verdade o endereço MAC do meu roteador local: 00:eb:d8:64:5d:21. Isso ocorre porque todo o tráfego da rede local é roteado através do meu roteador. O roteador usa um único endereço MAC para se comunicar com a Internet, e é esse endereço que aparece nas capturas de pacotes feitas no Wireshark. Portanto, em vez dos endereços MAC reais dos servidores da UFFS e da RNP, é visto o endereço MAC do roteador, que gerencia todas as conexões externas da rede local.