UNIVERSIDADE DO ESTADO DO AMAZONAS - UEA

GABRIEL FARACO

JACKSON KELVIN DE SOUZA

JULIANY RODRIGUES RAIOL

Relatório STMP

MANAUS-AM

2016

GABRIEL FARACO

JACKSON KELVIN DE SOUZA

JULIANY RODRIGUES RAIOL

Relatório SMTP

Trabalho solicitado pela professora Polianny, que ministra a disciplina de redes de computadores, para a composição de nota parcial.

MANAUS - AM

2016

SUMÁRIO

INTRODUÇÃO

O SMTP é o principal protocolo de camada de aplicação do correio eletrônico da Internet. Usa o serviço confiável de transferência de dados do TCP para transferir mensagens do servidor de correio remetente para o destinatário. Como acontece com a maioria dos protocolos da camada de aplicação, o SMTP tem dois lados: um lado cliente, que funciona no servidor de correio do remetente, e um lado servidor, que funciona no servidor de correio do destinatário. Ambos, o lado do cliente e o lado do servidor do SMTP, funcionam em todos os servidores de correio. Quando um servidor de correio envia correspondência para outros, age como um cliente SMTP. Quando o servidor de correio recebe correspondência de outros, age como um servidor SMTP.

1. Correio Eletrônico

Mais conhecido como ‘email’, funciona similarmente com o correio físico, pessoas enviam e recebem mensagens pela web, onde não é necessário que haja interação ao vivo entre as pessoas, seu uso independe do tempo online dos usuários. Um usuário envia uma mensagem para um usuário destinatário pela manhã, e esse apenas acessa a mensagem pela noite, é um exemplo. O email é rápido, fácil e barato de ser utilizado e é a aplicação de maior uso na internet.

2. STMP

2.1. Funcionamento

Para ilustrar a operação básica do SMTP, supondo que Alice queira enviar uma mensagem a Bob. Vamos ao exemplo:

1. Alice chama seu agente de usuário para e-mail, fornece o endereço de Bob (por exemplo, bob@uea.edu.br), compõe uma mensagem e instrui o agente de usuário a enviar a mensagem.
2. O agente de usuário de Alice envia a mensagem para seu servidor de correio, onde ela é colocada em um fila de mensagens.
3. O lado cliente do SMTP, que funciona no servidor do correio de Alice, vê a mensagem na fila e abre uma conexão TCP para um servidor SMTP, que funciona no servidor de correio de Bob. Caso o endereço de email do destinatário não seja válido, uma mensagem de notificação é enviada à Alice.
4. Após alguns procedimentos iniciais de apresentação (Handshaking), o cliente SMTP envia a mensagem de Alice para dentro da conexão TCP.
5. Se o servidor de correio de Bob não estiver em funcionamento, a mensagem permanece no servidor de correio de Alice esperando por uma nova tentativa. Ela não é adicionada a nenhum servidor de correio intermediário.

6. No servidor de correio de Bob, o lado servidor do SMTP recebe a mensagem e a coloca na caixa postal dele.
7. Bob chama seu agente de usuário para ler a mensagem quando for mais conveniente para ele por meio dos protocolos IMAP ou POP3.

2.2. Protocolos de acesso ao correio

Seguindo o exemplo anterior, quando o SMTP entrega a mensagem vinda do servidor de correio de Alice ao servidor de correio de Bob, ela é adicionada na caixa postal dele.

2.2.1. POP3

Por ser simples, sua funcionalidade é bastante limitada. Assim que baixar suas mensagens na máquina local, Bob pode criar pastas de correspondência e transferir as mensagens baixadas para elas. Em seguida, pode apagar as mensagens, mudá-las de pastas e procurar mensagens (por nome de remetente ou assunto). Mas esse paradigma – pastas e mensagem na máquina local – apresenta um problema para o usuário nômade que gostaria de manter uma hierarquia de pastas em um servidor remoto que possa ser acessado de qualquer computador: com o POP3, isso não é possível. Esse protocolo não provê nenhum meio para um usuário criar pastas remotas e designar mensagens à pastas.

O POP3 começa quando o agente de usuário (cliente) abre uma conexão TCP com o servidor de correio. Com a conexão TCP ativada, o protocolo passa por três etapas: autorização, transação e atualização. Durante a primeira etapa, autorização, o agente de usuário envia um nome de usuário e uma senha para autenticar o usuário. Na segunda etapa, transação, recupera as mensagens; é nessa etapa que o agente de usuário pode marcar as mensagens que devem ser apagadas, remover essas marcas e obter estatísticas de correio. A terceira etapa, atualização, ocorre após o cliente ter dado o comando QUIT que encerra essa sessão POP3 (nesse momento, o servidor de correio apaga as mensagens que foram marcadas).

2.2.2. IMAP

É um protocolo de acesso ao correio, porém com mais recursos, mas também significativamente mais complexo. (E, portanto, também as implementações dos lados cliente e servidor são significativamente mais complexas.)

Um servidor IMAP associa cada mensagem a uma pasta. Quando uma mensagem chega a um servidor pela primeira vez, é associada com a pasta INBOX do destinatário, que, então, pode transferir a mensagem para uma nova pasta criada por ele, lê-la, apagá-la e assim por diante. O protocolo IMAP provê comandos que permitem que os usuários criem pastas e transfiram mensagens de uma para outra. O protocolo também provê comandos que os usuários podem usar para pesquisar pastas remotas em busca de mensagens que obedeçam a critérios específicos.

3. Aspectos investigativos

Para a elaboração do trabalho utilizou-se duas ferramentas: o Wireshark, que é um analisador de protocolo de tráfego de rede, e o Thunderbird, um cliente de emails. O wireshark recebia a movimentação da rede a partir de alguma atividade, leitura ou escrita de emails, realizada no Thunderbird.

O Thunderbird foi escolhido pois via browser não é possível verificar o tráfego dos protocolos de correio eletrônico, apenas o HTTP.

3.1.Filtros no WireShark

Um dos atrativos do wireshark é a facilidade de criar filtros para os pacotes capturados. Essa aplicação é útil para a análise do tráfego de rede.

Exemplo de alguns filtros que foram utilizadas para a visualização de dados de um protocolo:

- Protocolo SMTP: tcp.port == 465
- Protocolo IMAP: tcp.port == 993

- Protocolo POP3: tcp.port == 995

3.2. Processo de investigação

O processo de investigação foi dividido em duas partes: Configuração da conta de e-mail e Configuração da conta de E-mail no cliente do Thunderbird. Após isso, foi realizado procedimentos diretamente no Wireshark, para a visualização dos dados.

3.2.1. Configuração da conta de E-mail

O primeiro passo é o configurar a conta do conta no Gmail. Deve-se ir na seção "Minha conta" e, após isso, ir em "Login e segurança". Nesta parte, é preciso permitir que o Thunderbird, ou outro aplicativo cliente, tenha acesso ao E-mail.

Figura 1: Conta de E-mail.

A imagem abaixo é a tela que será exibida após o botão "Minha conta" tiver sido selecionado.

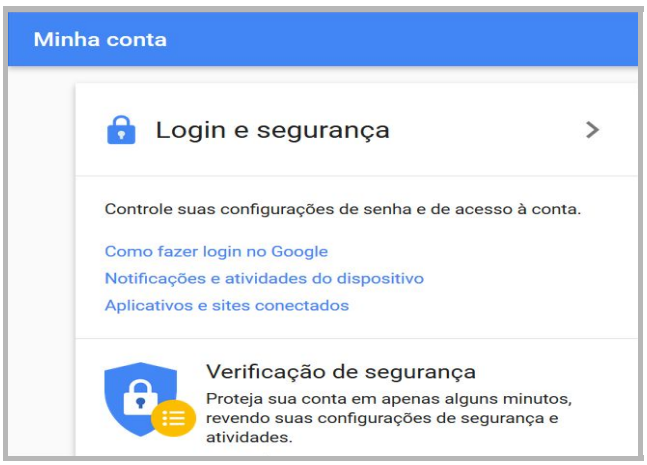

Figura 2: Minha conta.

A imagem abaixo é a tela que será exibida após o botão “Aplicativos e sites conectados” tiver sido selecionado.

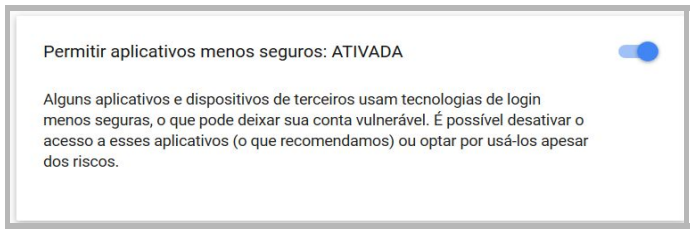

Figura 3:Login e segurança.

3.3.Configuração da conta de E-mail no cliente do Thunderbird

Insira os dados requeridos, em seguida escolha o protocolo de acesso ao correio desejado, IMAP ou POP3.

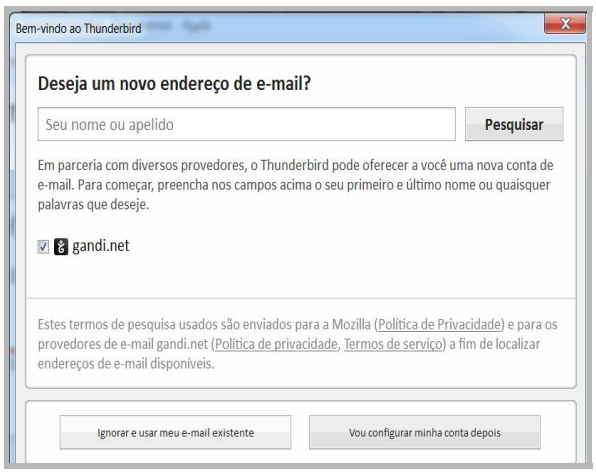

Figura 4:Login e segurança.

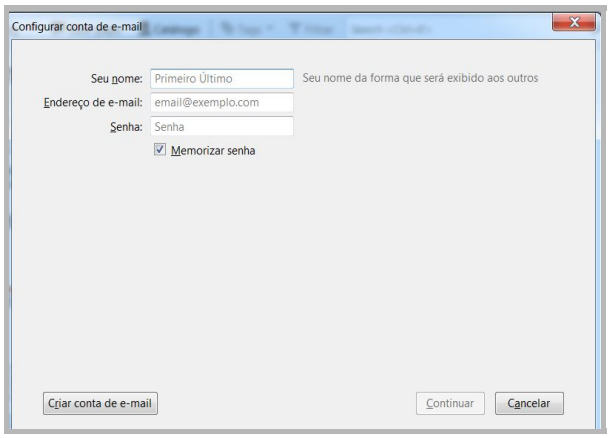

Figura 5:Login e segurança.

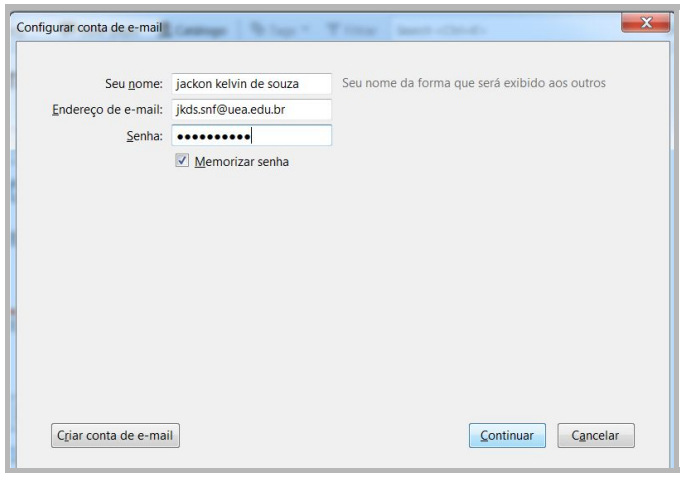

Figura 6:Login e segurança.

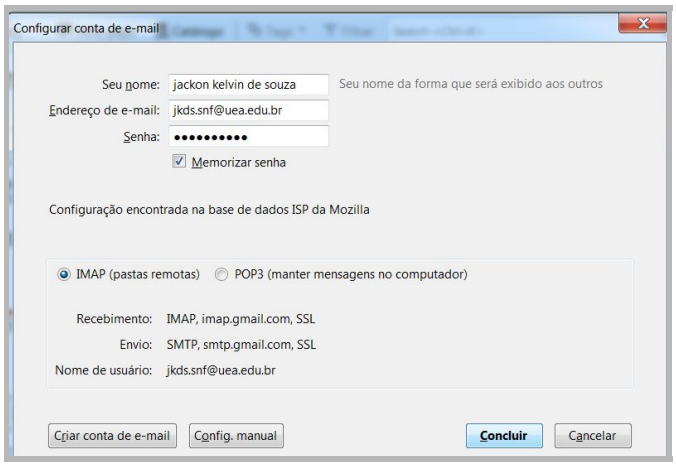

Figura 7:Login e protocolo de acesso ao correio.

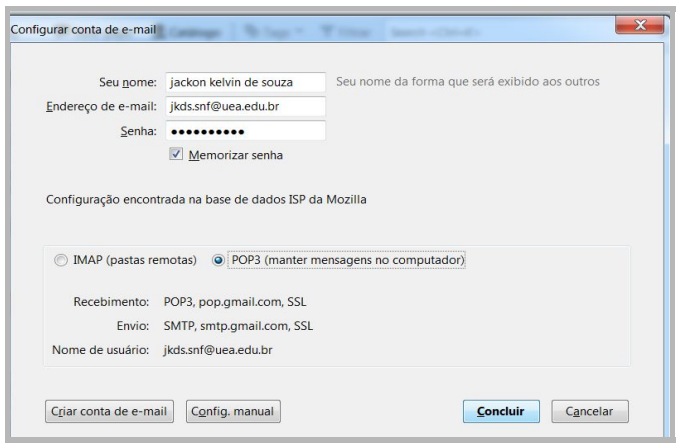

Figura 8:Login e protocolo de acesso ao correio.

3.4. Resultados obtidos

Partindo da configuração do Thunderbird, usou-se dos recursos de filtros do Wireshark para analisar o tráfego de rede. A seguir, é possível visualizar os passos para a obtenção de pacotes dos protocolos SMTP, IMAP e POP3.

3.4.1. Protocolo SMTP

Nas configurações da conta do E-mail no Thunderbird é possível visualizar o número da porta que o Gmail usa no protocolo SMTP.

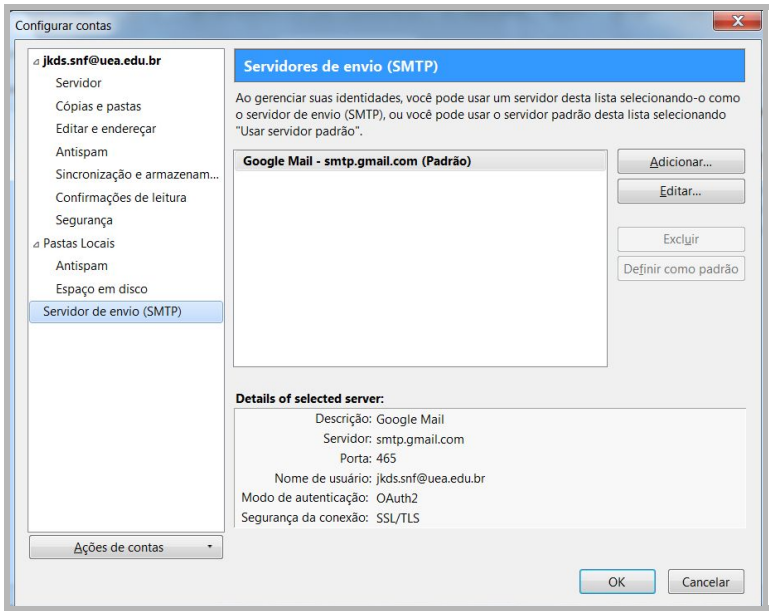

Figura 9: Protocolo SMTP default do Gmail no Thunderbird.

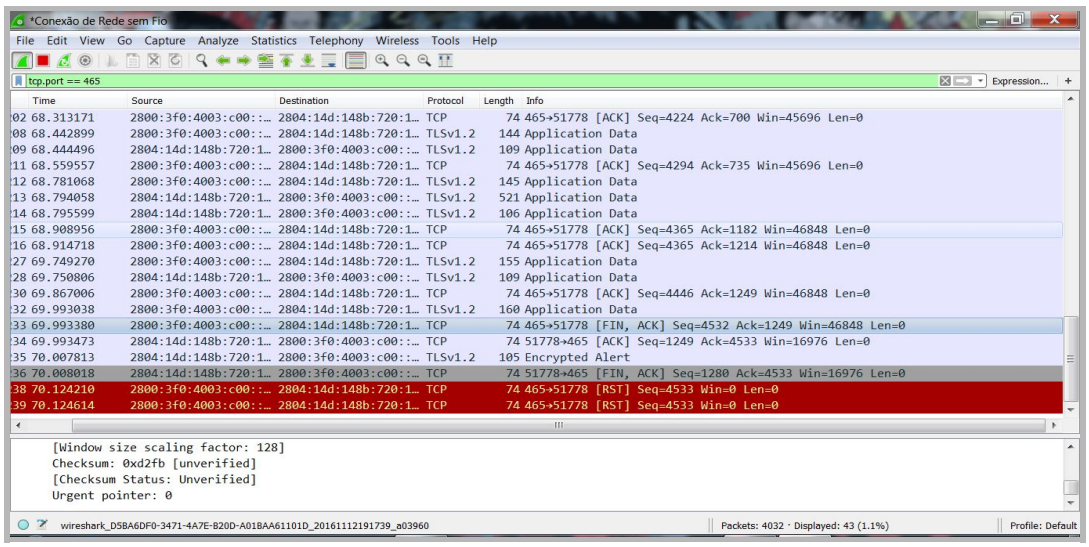

Figura 10: Recebimento e Visualização de pacotes do protocolo SMTP no Wireshark.

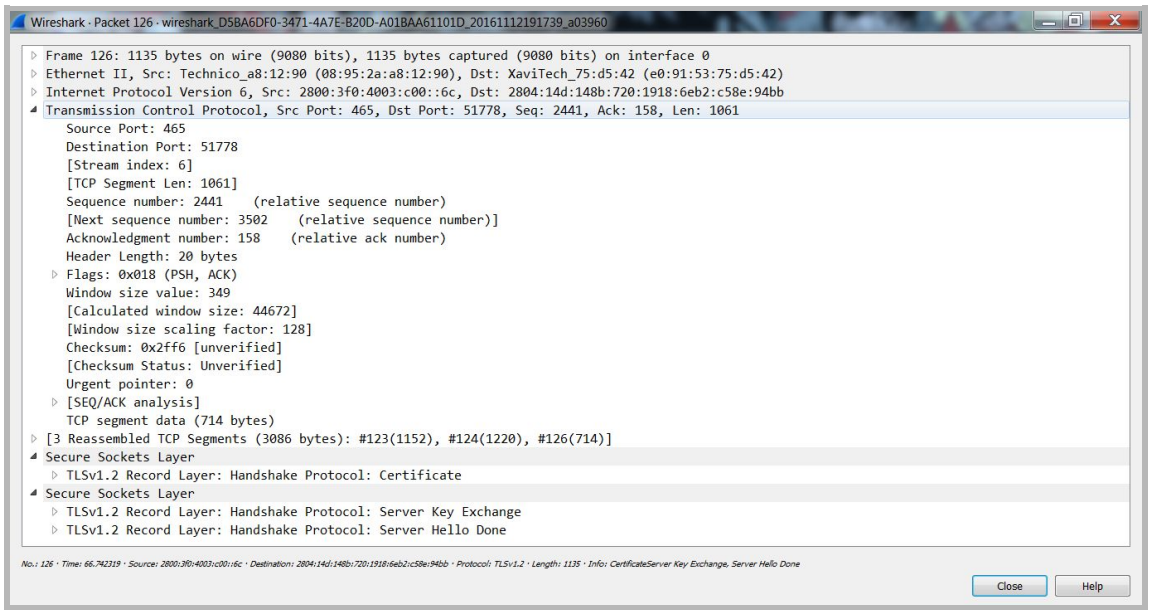

Figura 11: Recebimento e Visualização de pacotes do protocolo SMTP no Wireshark.

Na figura 11, é possível visualizar a o Handshake entre o remetente e destinatário, e na figura 12, é possível visualizar a mensagem criptografada.

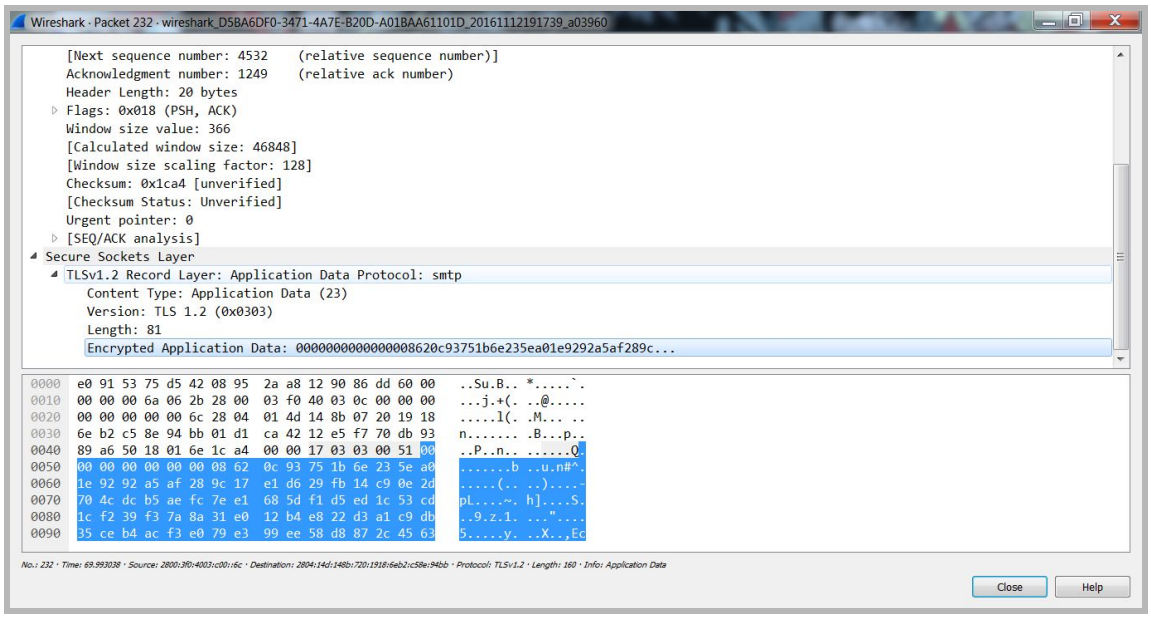

Figura 12: Mensagem criptografada.

3.4.2. Protocolo IMAP

Nas configurações da conta do E-mail no Thunderbird é possível visualizar o número da porta que o Gmail usa no protocolo IMAP.

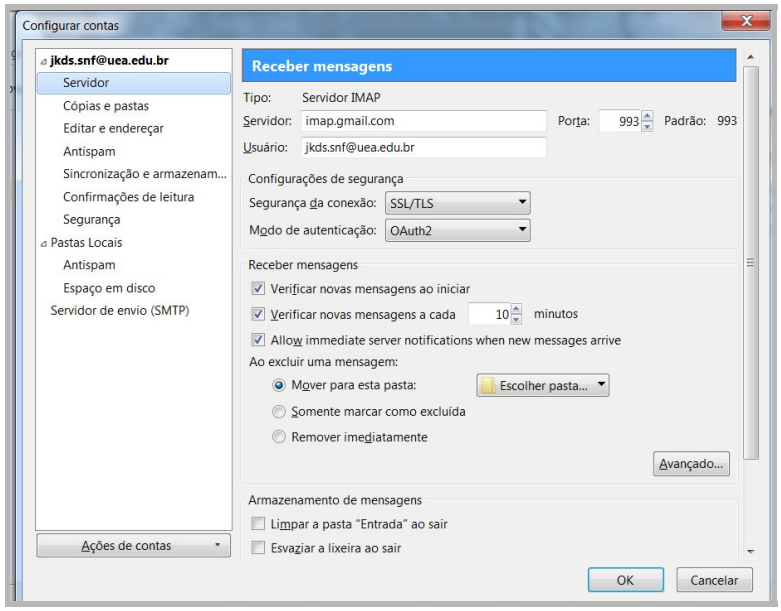

Figura 13: Protocolo IMAP default do Gmail no Thunderbird.

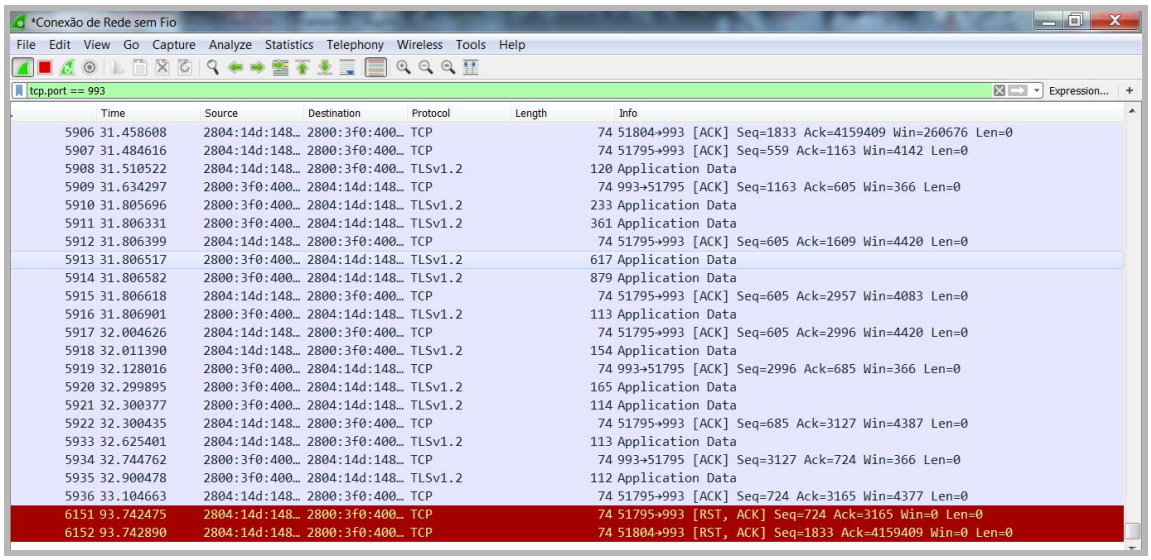

Figura 14: Recebimento e Visualização de pacotes do protocolo IMAP no Wireshark.

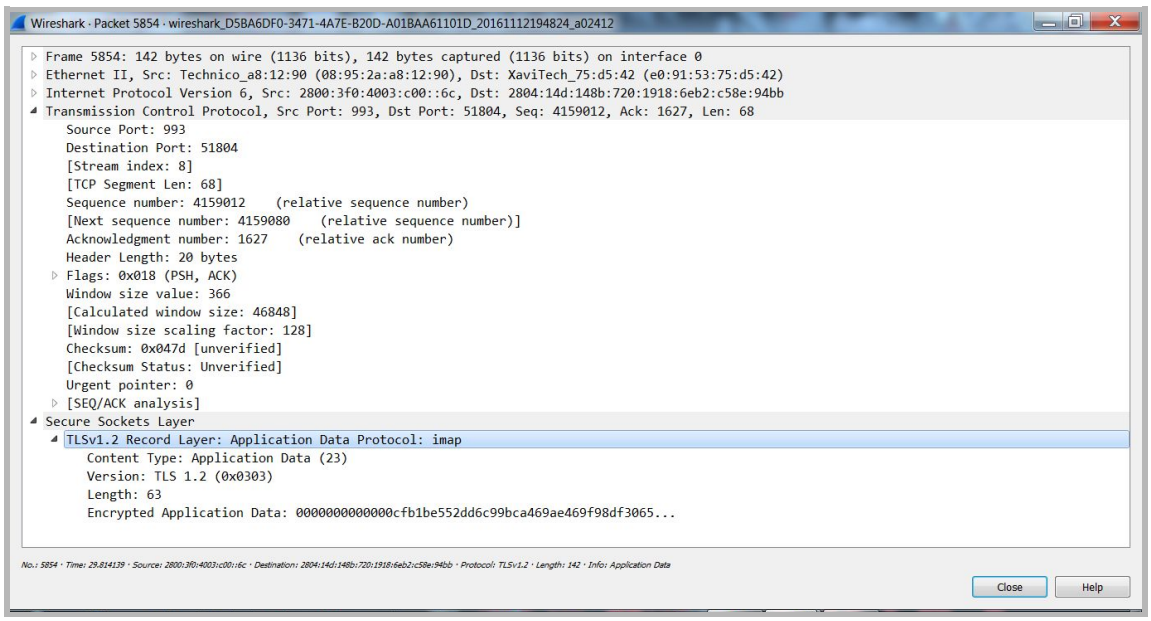

Figura 15: Recebimento e Visualização de pacotes do protocolo SMTP no Wireshark.

Na figura 15, é possível visualizar a mensagem criptografada.

3.4.3. Protocolo POP3

Nas configurações da conta do E-mail no Thunderbird é possível visualizar o número da porta que o Gmail usa no protocolo POP3.

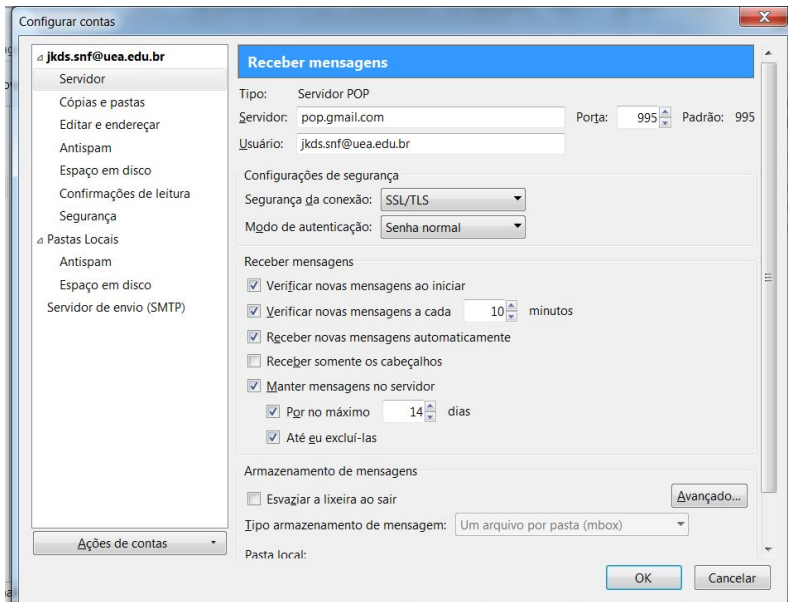

Figura 16: Protocolo POP3 default do Gmail no Thunderbird.

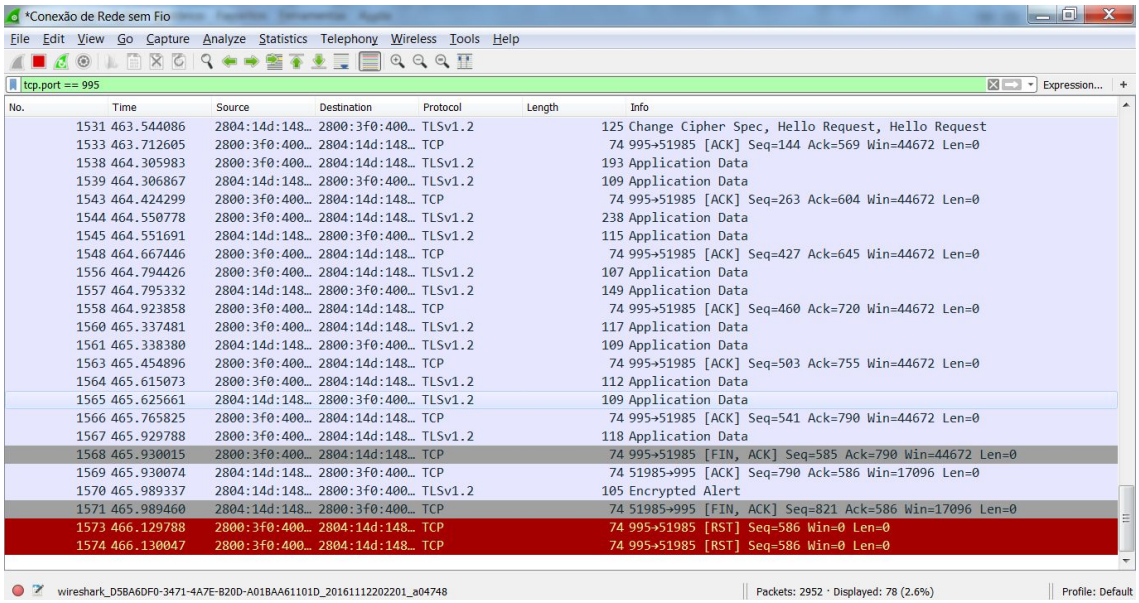

Figura 17: Recebimento e Visualização de pacotes do protocolo POP3 no Wireshark.

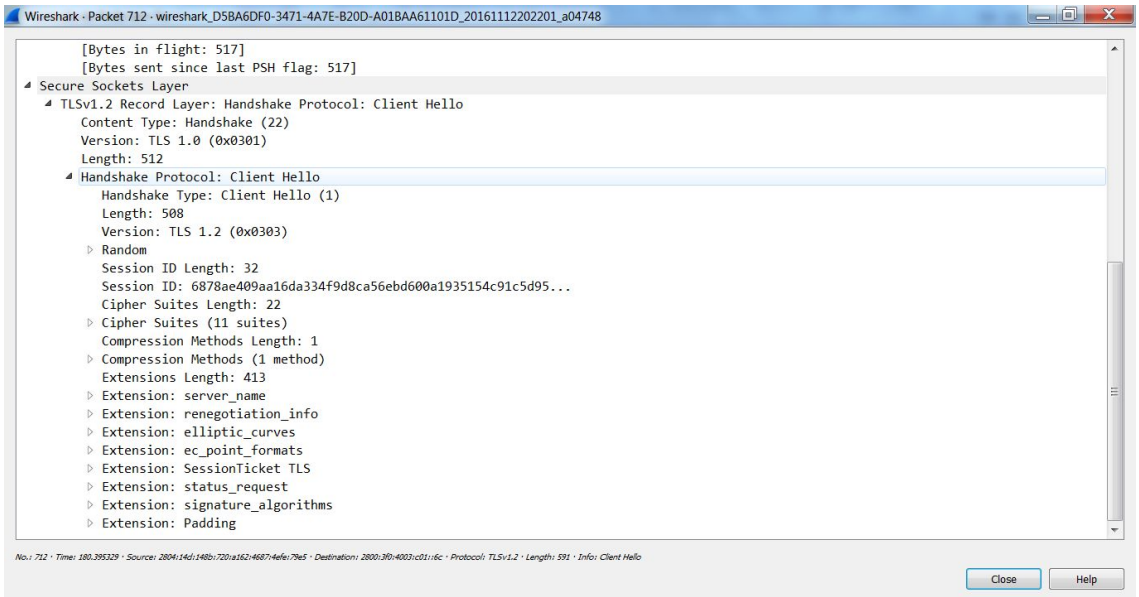

Figura 18: Recebimento e Visualização de pacotes do protocolo POP3 no Wireshark.

4. Conclusão

O Wireshark é uma ferramenta poderosa para detectar problemas e entender melhor o funcionamento de cada protocolo, e não necessita de nenhuma configuração complexa para seu funcionamento. Ele analisa o tráfego de rede, e o organiza por protocolos e com a possibilidade da utilização de filtros, sendo assim possível controlar o tráfego de uma rede e saber tudo o que entra e sai do computador, em diferentes protocolos, ou da rede à qual o computador está ligado.

5. Referências

KUROSE, James F; ROSS, Keith W. *Redes de computadores e a Internet - uma abordagem top-down.* 5 ed. São Paulo: Addison Wesley, 2010.

TANENBAUM, Andrew S; WETHERALL, David. *Redes de computadores.* 5 ed. São Paulo: èarson Prentice Hall, 2011.