UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

SISTEMAS INFORMATICOS Y COMPUTACION

COMPONENTE: ARQ Y SEGURIDAD DE REDES

ESTUDIANTE: Luis Alfredo Jaramillo Uday (1719626754)

DOCENTE: Romel Vicente Torres Tandazo

TEMA: “SMTP”

FECHA DE ENTREGA: 09-11-2020

LOJA-ECUADOR

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA
La Universidad Católica de Loja
TITULACIÓN: SISTEMAS INFORMÁTICOS Y COMPUTACIÓN

PRACTICA #2: CORREO ELECTRÓNICO	
PERIODO ACADÉMICO:	OCT/2018 – FEB/2019
COMPONENTE:	ARQUITECTURA Y SEGURIDAD DE REDES
TITULACIÓN	SISTEMAS INFORMÁTICOS Y COMPUTACIÓN
PARALELO:	A y B
DOCENTE:	Ing. Javier F. Martínez, Mgs
OBJETIVO GENERAL	Comprender las funciones de capa de aplicación y sus servicios
OOBJETIVOS ESPECÍFICOS	• Describir los diferentes protocolos de correo electrónico SMTP Y POP3 • Diferenciar el funcionamiento y uso de los distintos protocolos permiten el intercambio de correos electrónicos.

1. |ACTIVIDADES

- Instalación del servidor de correo electrónico para Windows hmailserver y el cliente de telnet PuTTy.
- Creación del dominio del correo electrónico y cuentas para realizar pruebas.
- Monitoreo del tráfico de red en el servidor por medio de WIRESHARK

2. COMANDOS DE CORREO ELECTRÓNICO

SMTP

El protocolo SMTP es el protocolo básico que utilizan los servidores de correo para enviarse mensajes entre sí. Está descrito en el documento RFC 5321 y utiliza mensajes en formato ASCII de 7 bits. Esto incumbe tanto a los comandos, como a las cabeceras y al cuerpo de los mensajes. El protocolo SMTP utiliza el **puerto 25**. La siguiente tabla lista algunos de los comandos que incluye.

Comando	Descripción
HELO	Identificación del cliente, generalmente con un nombre de dominio.
EHLO	Permite al servidor declarar su aceptación de comandos ESMTP (Extended
MAIL FROM	Emisor del mensaje.
RCPT TO	Receptor(es) del mensaje.
TURN	Permite al cliente y al servidor invertir los roles y enviarse mensajes en
ATRN	Authenticated TURN. Tiene como parámetros opcionales uno o más dominios. Debe ser rechazado si la sesión no ha sido
SIZE	Proporciona un mecanismo por el que el servidor SMTP puede indicar el máximo tamaño de mensaje admitido. Un cliente no debe enviar mensajes de mayor tamaño que el indicado por el servidor.
ETRN	Es una extensión de SMTP. ETRN lo envía un servidor SMTP para solicitar a otro servidor el envío de los mensajes que tenga.

PIPELINING	Permite enviar una sucesión de comandos encadenados sin esperas de
DATA	Lo envía el cliente para indicar que inicia el envío del contenido del mensaje.
DSN	Comando ESMTP que habilita el envío de notificaciones de estado del envío
RSET	Anula la transacción completa y reinicializa el buffer.
VRFY	Verifica que un buzón existe. Por ejemplo, 'VRFY Ted' verifica que el buzón
HELP	Devuelve una lista de comandos admitidos por el servidor SMTP.
QUIT	Finaliza la sesión.

Transacción de ejemplo:

```
HELO arquiredes.net
>250 arquiredes.net
AUTH LOGIN (se ingresan usuario y contraseña en
codificación base64 https://www.base64encode.org/
)
MAIL FROM: pepe@pepito.es
>250 2.1.5. OK
RCPT TO: usuario@servidor.es
>250 2.1.5. Ok
DATA
>354 Start mail input; endi with <CRLF>.<CRLF>
subject: Asunto
Este mensaje es de prueba.
Probamos el protocolo SMTP.

>250 2.0.0 OK: queued as 6D126A066
QUIT
>221 2.0.0 Bye
```

POP3

El protocolo POP está definido en el RFC 1939. Tiene 3 fases de funcionamiento. En la primera, la autenticación, el cliente envía los comandos USER y PASS uno a continuación del otro, y se identifica como usuario autorizado. La segunda fase, la transacción, sirve para que el cliente recupere los mensajes. Opcionalmente, también marcará mensajes para borrar. La última fase, la actualización, tiene lugar cuando el cliente ha terminado la sesión, y en ella se borran los mensajes marcados para borrado. Las comunicaciones se realizan por medio de comandos ASCII. La siguiente tabla lista algunos de los comandos más usados.

Comando	**Descripción**
USER <usario>	Nombre de usuario
PASS <contraseña>	Contraseña
QUIT	Finalizar sesión
STAT	Número de mensajes y tamaño total.
LIST <n de mensaje>	Número del mensaje y su tamaño. Si no se proporciona número de mensaje, lista todos.
RETR n de mensaje	Descargar mensaje
DELE n de mensaje	Borrar mensaje
TOP mensaje líneas	Muestra las primeras "líneas" líneas del mensaje número "mensaje". Incluye la cabecera.
NOOP	No-operación

RSET	Deshace los cambios hechos en la sección, incluido el borrado de mensajes.

Transacción de ejemplo:

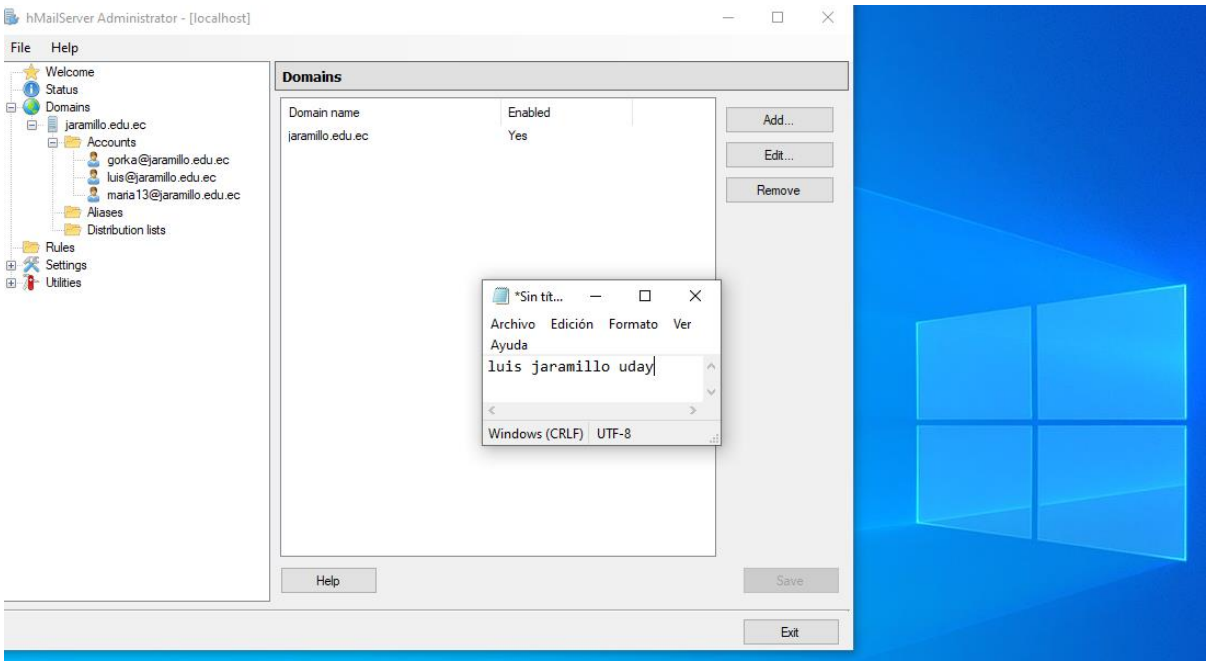
```
USER pepe
>+OK Ñame is a valid mailbox
PASS LaContrasenia
>+OK Mailbox locked and ready
LIST
>+OK sean listing follows
>1 23941
>2 2411
>3 16523
>4 892034
RETR 1 (Recupera el mensaje 1 )
QUIT
>+OK
```

De nuevo, las líneas que empiezan por > son las respuestas del servidor. El ejemplo presupone la conexión telnet con el puerto 110 del servidor POP3.

3. DESARROLLO DE LA PRÁCTICA

Primeramente por parte del docente se hará un pequeño tutorial explicando el funcionamiento de hMailServer y PuTTy. Luego los grupos de estudiantes realizarán las actividades expuestas a continuación.

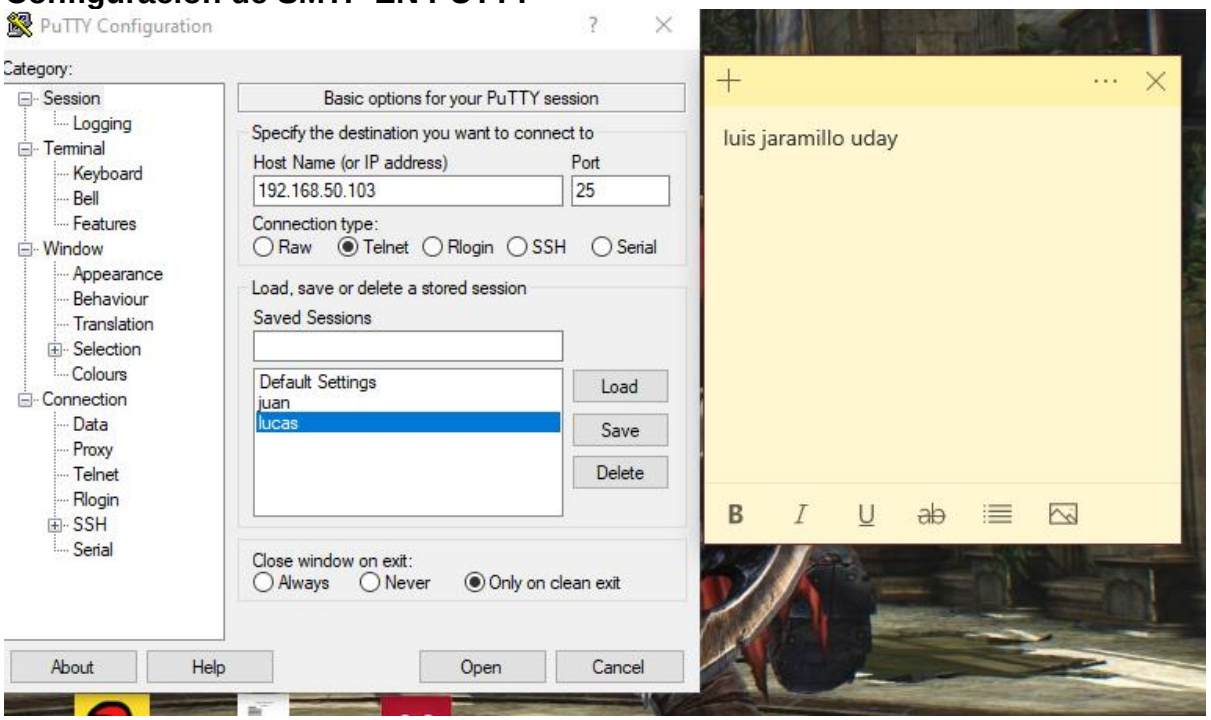
Instalar hMailServer y el cliente telnet PuTTy en su PC. Configurar un dominio de correo electrónico con el nombre del grupo por ejemplo (nombregrupo.net). Crear cuentas de correo para cada integrante del grupo. Por cada grupo solo debe haber un servidor de correo.



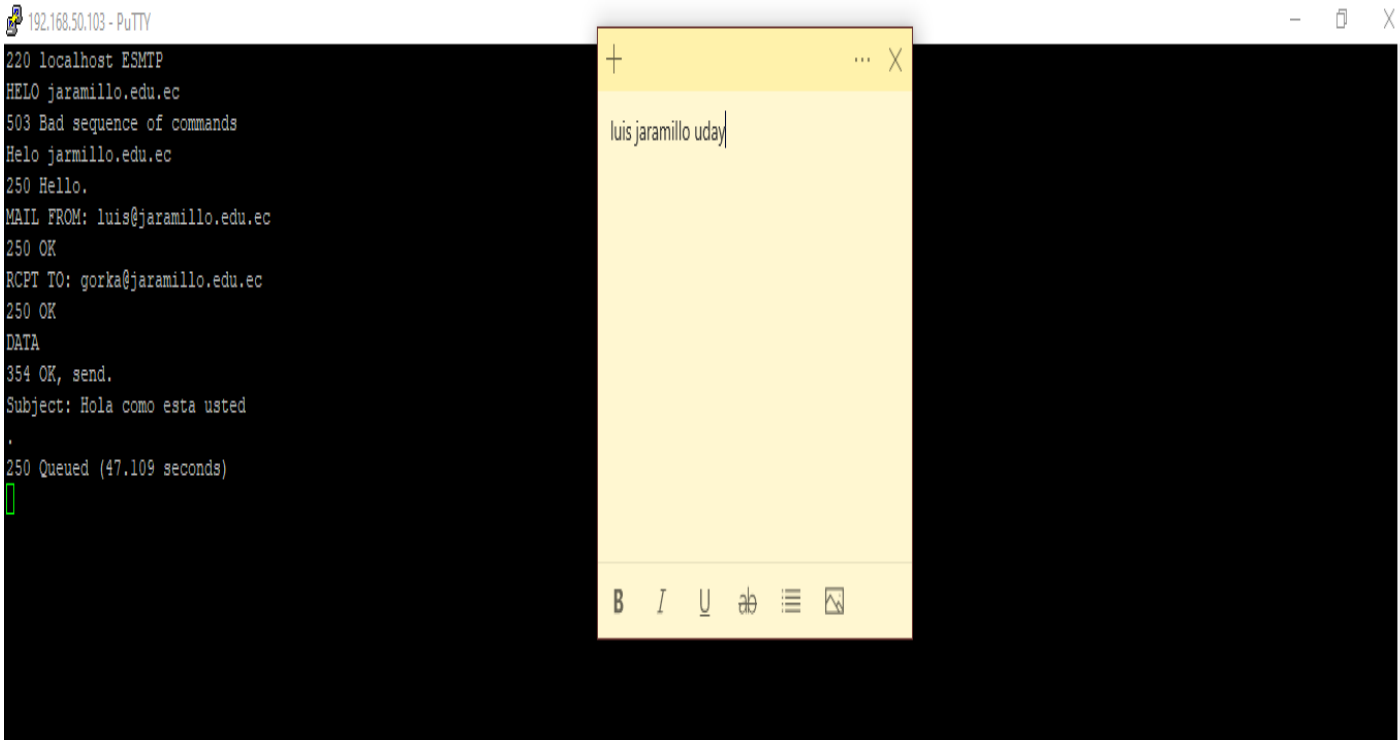
Por cada transacción se deberá sniffear el tráfico en el servidor, y realizar el filtro con SMTP o POP dependiendo la transacción realizada. **Realizar cada transacción una por vez y analizar los paquetes.**

Enviar correos de prueba entre los integrantes del grupo por pares usando el cliente PuTTy y usando SMTP. Luego recuperar los mensajes usando el protocolo POP3 y PuTTy. **Realizar el diagrama de mensajes del envío y recuperación de los mensajes, entre servidor y cliente.**

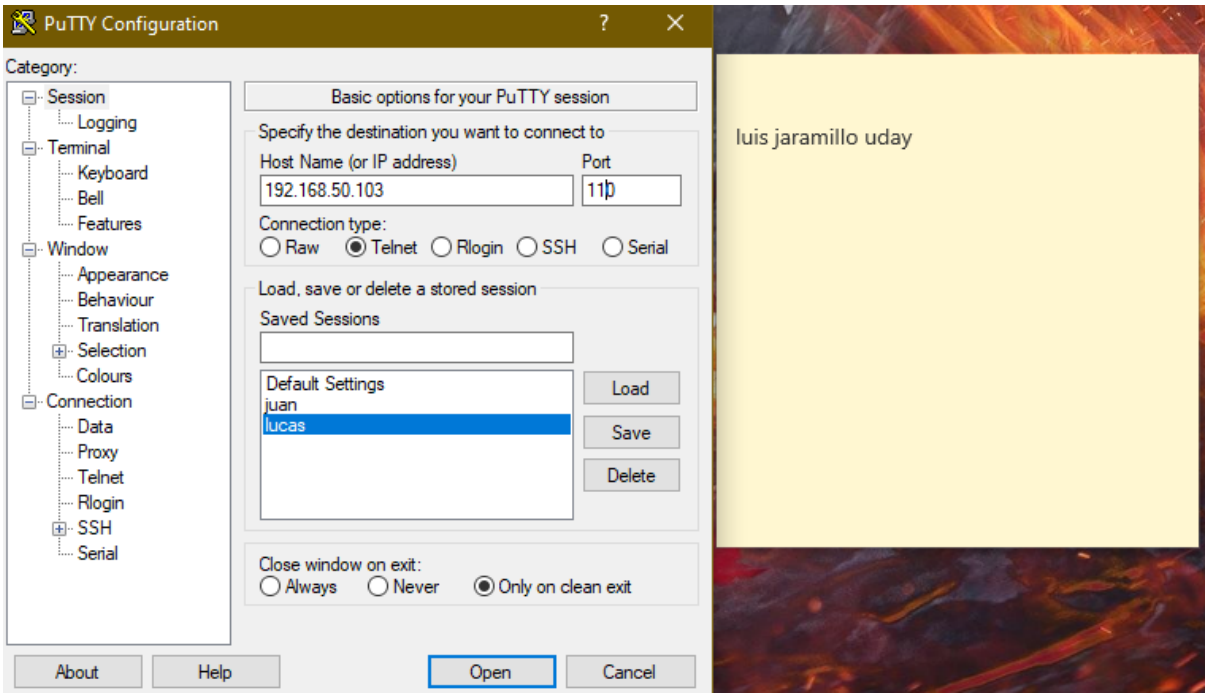
Configuración de SMTP EN PUTTY



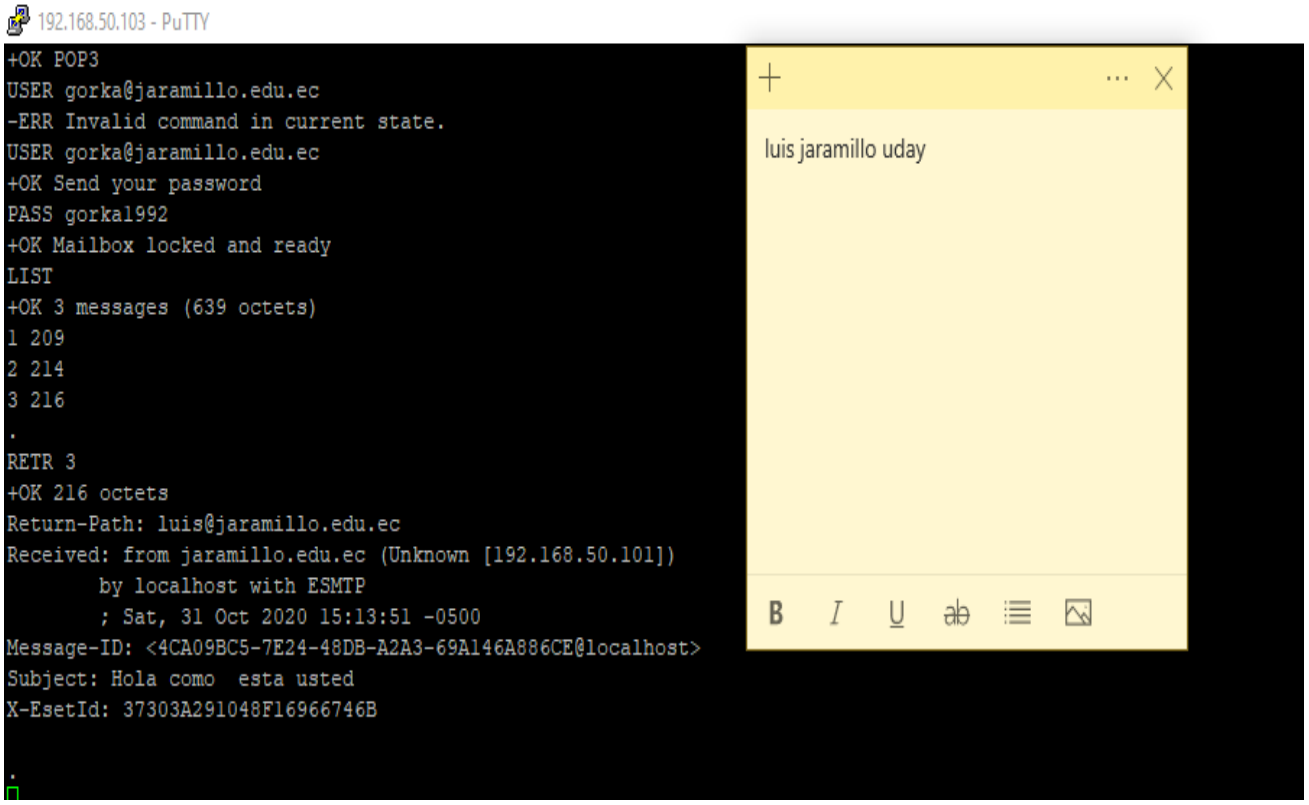
Interacción de comandos smtp en putty



Configuración de POP EN PUTTY



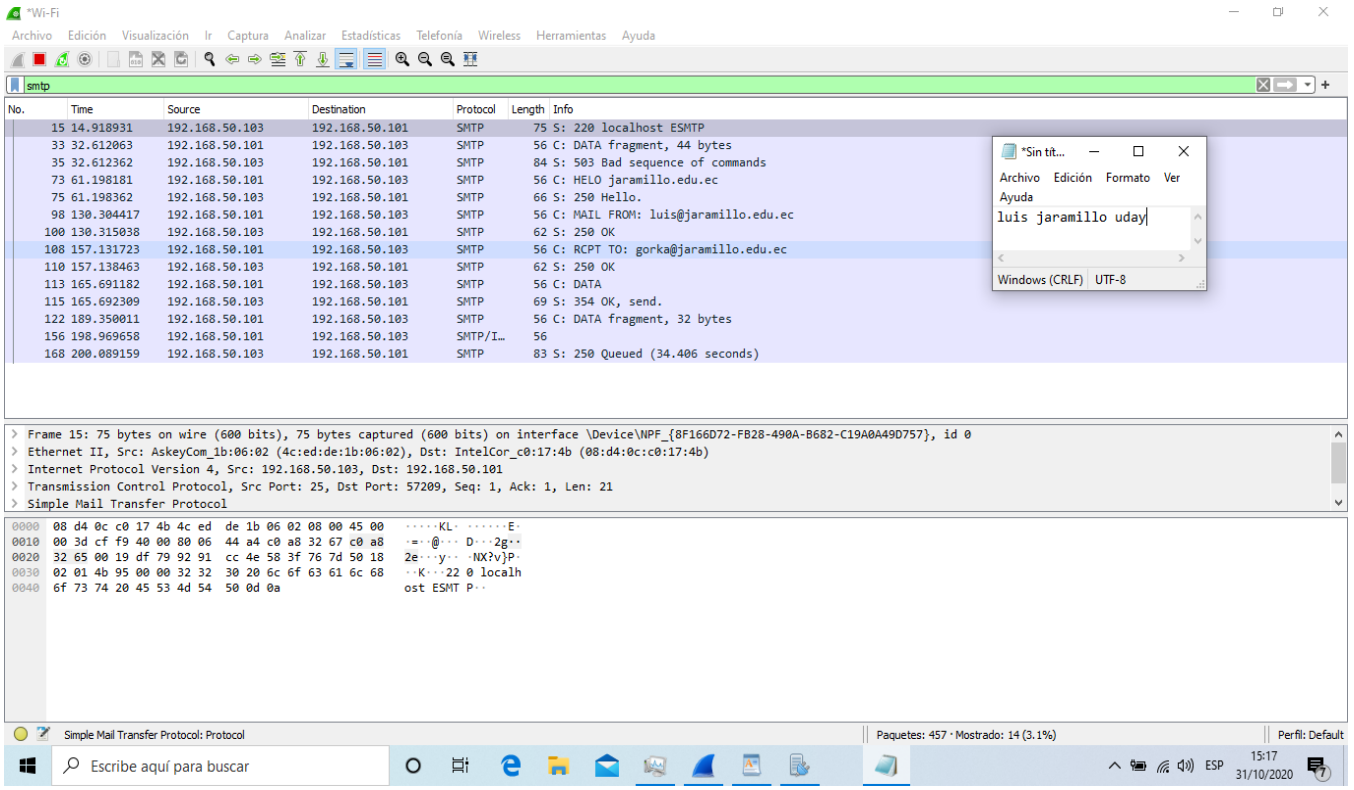
Interacción de comandos smtp en putty



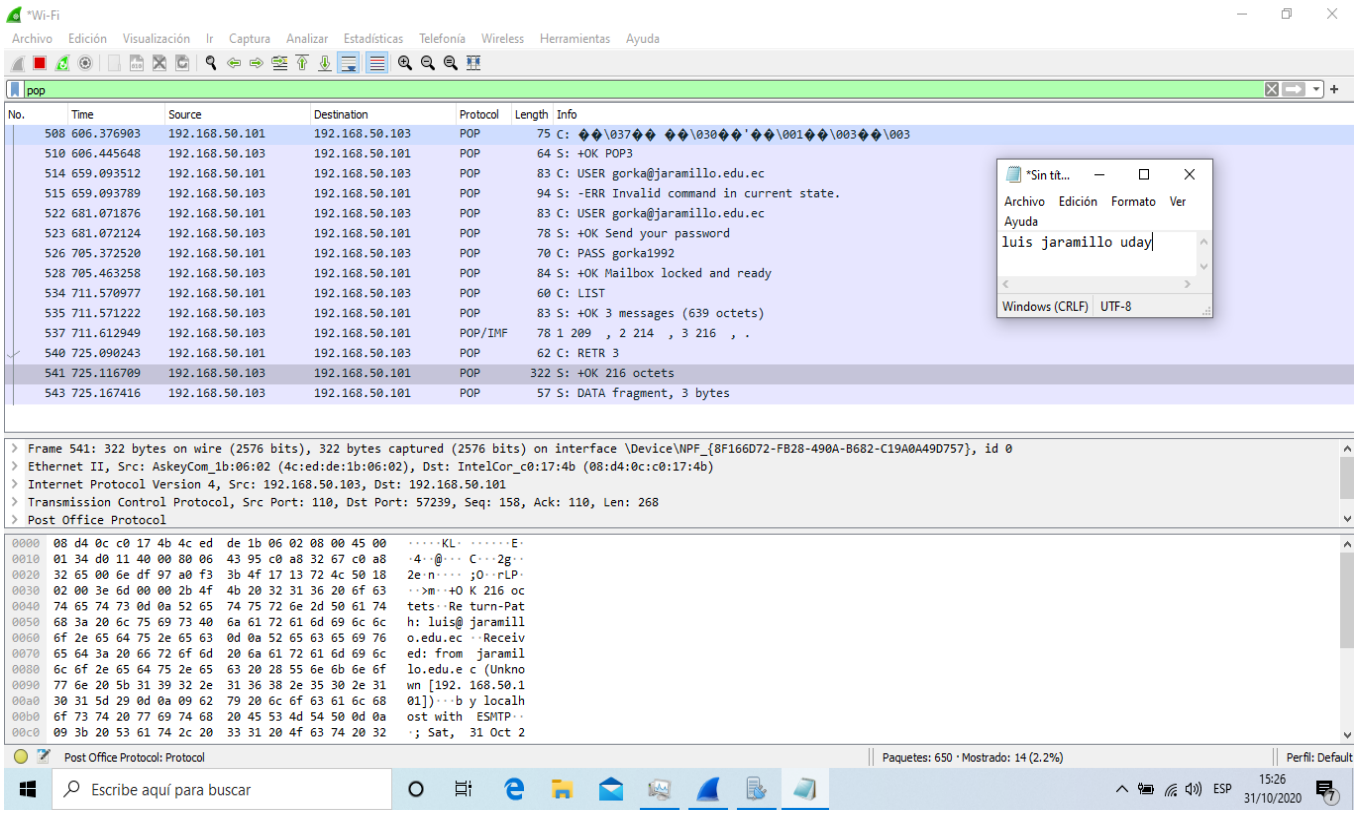
Responder las siguientes incógnitas:

¿Qué información se pudo obtener al sniffear los paquetes?
Inicialmente se puede obtener todos los comandos realizados desde PuttY

Interacción en wherishark de SMTP



Interacción en wherishark de POP



- Además, se puede obtener la información de los mensajes enviados.

¿Debido a que se puede obtener los usuarios y contraseñas?
Con el protocolo por se puede llegar a obtener los usuarios y contraseñas de los que realizan la consulta de los mensajes porque POP3 es un protocolo un poco antiguo por lo que utiliza aún un mecanismo de firmado sin cifrado, por ello la transmisión de contraseñas de POP3 en texto plano es común.

¿Se puede leer el contenido de los correos al sniffear?
Si se puede leer el contenido de los correos tanto al enviar los correos como para listarlos.