**Capa de Aplicación - Correo electrónico Redes y comunicaciones - 2022**

**Práctica 4**

**Capa de Aplicación - Correo electrónico**

**Correo electrónico**

**10 11 12**

**1. ¿Qué protocolos se utilizan para el envío de mails entre el cliente y su servidor de correo? ¿Y entre**

**servidores de correo?**

Para enviar un correo, se usa un agente de usuario que lo manda al servidor de correo. Esta transferencia de información se puede lograr haciendo uso de SMTP.

● **SMTP:** Es un protocolo de comunicaciones basado en texto. Limitaciones en cuanto a la recepción de mensajes en el servidor de destino (cola de mensajes recibidos), por las que se asocia con otros protocolos, como el POP o IMAP, otorgando a **SMTP** la tarea específica de **enviar correo**, y recibirlos empleando los otros protocolos antes mencionados (POP O IMAP).

● **HTTP:** Cuando se utiliza un navegador para enviar correos, se utiliza como protocolo HTTP. Sin embargo, no debe considerárselo como protocolo para correo electrónico, ya que solo es el protocolo usado para llegar hasta el servidor de correo. Luego, la aplicación a la cual nos conectamos va a utilizar protocolos SMTP para enviar mails, y POP3 o IMAP para recibir mails. Si usamos un cliente de correo, no se va a utilizar HTTP.

● **ESMTP:** la versión segura de SMTP.

El protocolo que siempre se utiliza para la comunicación entre los servidores de correo es SMTP o ESMTP.

**2. ¿Qué protocolos se utilizan para la recepción de mails? Enumere y explique características y diferencias entre las alternativas posibles.**

Para leer los correos se debe utilizar un agente de usuario el cual se comunicará con el servidor de correo a través de algunos de los siguientes protocolos:

● **POP3:** (Post Office Protocol -- Version 3) es un protocolo de acceso de correo simple con funcionalidad limitada. Comienza cuando el agente de usuario abre una conexión TCP hacia el servidor de correo en el puerto 110. Con la conexión TCP establecida, POP3 avanza a lo largo de 3 fases:

* Autorización: El agente de usuario envía username y contraseña.
* Transacción: El agente de usuario recibe mensajes y el usuario puede marcar correos para borrado.
* Actualización: Luego de que el usuario utiliza el comando quit, el cual finaliza la sesión POP3; en este momento el servidor de mail elimina los correos marcados.

Descarga los mails en la PC, donde quedan almacenados. Una vez hecho esto, los correos sólo serán accesibles desde la PC donde se bajaron, ya que se eliminan del servidor. (configuración descarga-borrado. También existe la configuración descarga-almacenamiento, la cual deja los mails en el servidor.)

Útil si se usa siempre la misma PC. Se puede acceder a los correos ya descargados si no hay internet.

● **IMAP:** Protocolo de acceso de correo. Mas características y complejidad que POP3. Asocia cada mensaje con una carpeta; cuando un mensaje arriba al servidor es asociado con la carpeta INBOX del receptor, quien puede mover, leer o eliminar el mensaje.

Tiene comandos para obtener solamente el header del mensaje o una parte de un mensaje MIME. Esto es útil cuando la conexión tiene poco ancho de banda. IMAP no descarga los mensajes a la PC: tanto los mensajes como las carpetas se mantienen en el servidor, lo que es ventajoso si se usan diferentes dispositivos, pero debe considerarse que puede agotarse el espacio.

También brinda más seguridad si se usa una PC compartida, ya que no almacena información en la máquina local. El inconveniente de este protocolo es que siempre hemos de disponer de conexión a internet.

● **HTTP:** Cuando se utiliza navegador web como agente de usuario para la recepción de correos, éste utilizará el protocolo HTTP para comunicarse con el servidor de correo. Sin embargo, el servidor de correo debe usar los protocolos antes mencionados.

|  |  |  |
| --- | --- | --- |
|  | **POP** | **IMAP** |
| **Almacenamiento de correos** | Temporal en un servidor (por default), permanente en los clientes | Servidor externo principalmente |
| **Mantenimiento de sincronía entre clientes** | Difícil | Fácil |
| **Estabilidad** | Baja | Alta |
| **Organización, en el servidor** | Único buzón de entrada para todos los correos | Se pueden crear subcarpetas |
| **Organización, en los clientes** | Se pueden crear subcarpetas | Se pueden crear subcarpetas |
| **Internet** | No necesita para leer lo que ya se descargó | Siempre se necesita para acceder |

**3. Utilizando la VM y teniendo en cuenta los siguientes datos, abra el cliente de correo (thunderbird) y**

**configure dos cuentas de correo. Una de las cuentas utilizará POP para solicitar al servidor los mails**

**recibidos para la misma mientras que la otra utilizará IMAP.**

**Al crear cada una de las cuentas, seleccionar Manual config y luego de configurar las mismas según lo**

**indicado, ignorar advertencias por uso de conexión sin cifrado.**

**Datos para POP**

**Cuenta de correo: alumnopop@redes.unlp.edu.ar**

**Nombre de usuario: alumnopop**

**Contraseña: alumnopoppass**

**Puerto: 110**

**Datos para IMAP**

**Cuenta de correo: alumnoimap@redes.unlp.edu.ar**

**Nombre de usuario: alumnoimap**

**Contraseña: alumnoimappass**

**Puerto: 143**

**Datos comunes para ambas cuentas**

**Servidor de correo entrante (POP/IMAP):**

**• Nombre: mail.redes.unlp.edu.ar**

**• SSL: None**

**• Autenticación: Normal password**

**Servidor de correo saliente (SMTP):**

**• Nombre: mail.redes.unlp.edu.ar**

**• Puerto: 25 (EL puerto SMPT)**

**• SSL: None**

**• Autenticación: Normal password**

**Puerto 587 usado por el MSA.**

**a. Verificar el correcto funcionamiento enviando un email desde el cliente de una cuenta a la otra y**

**luego desde la otra responder el mail hacia la primera.**

**b. Análisis del protocolo SMTP**

**i. Utilizando Wireshark, capture el tráfico de red contra el servidor de correo mientras desde la**

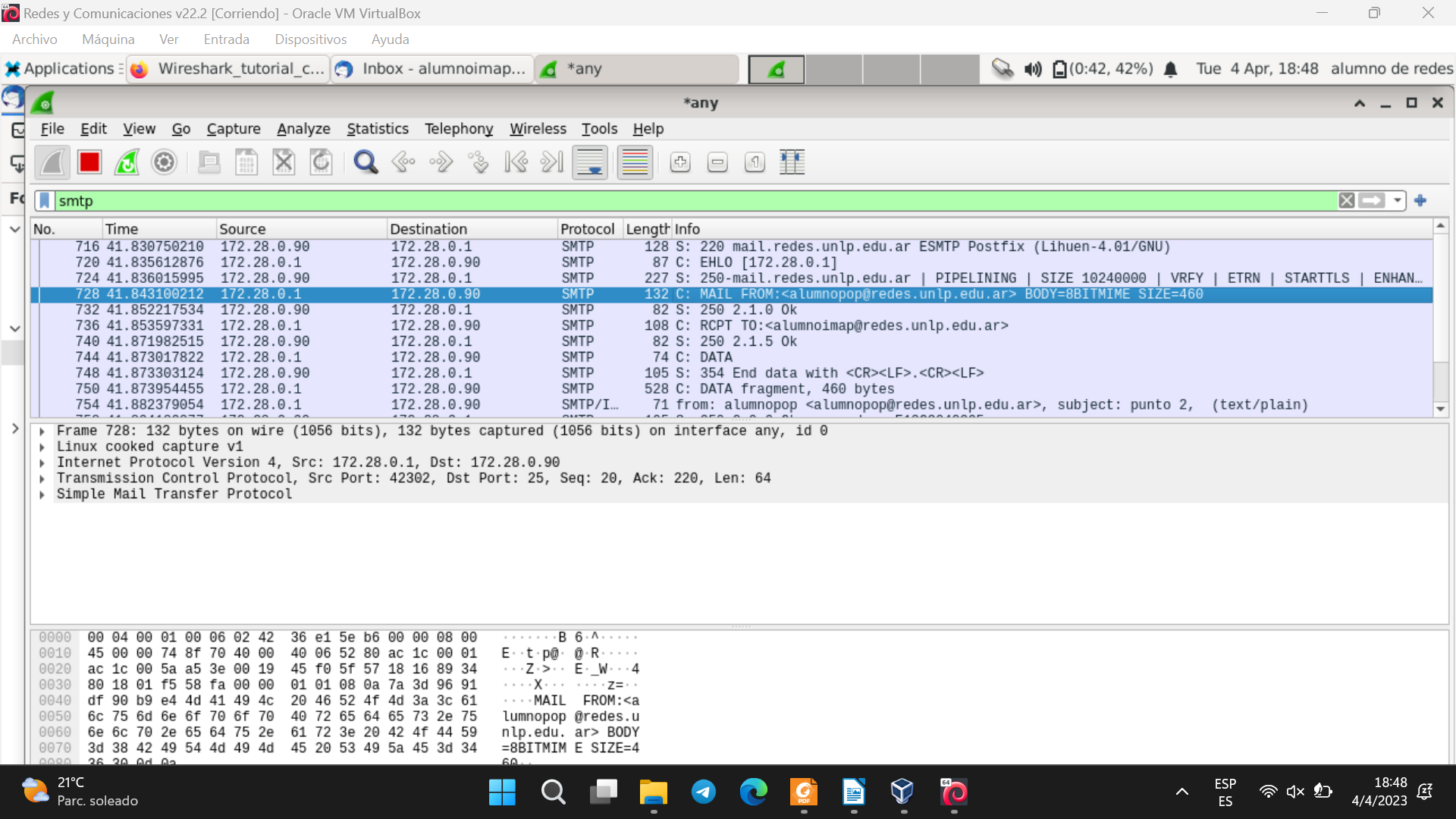
**cuenta alumnopop@redes.unlp.edu.ar envía un correo a alumnoimap@redes.unlp.edu.ar**

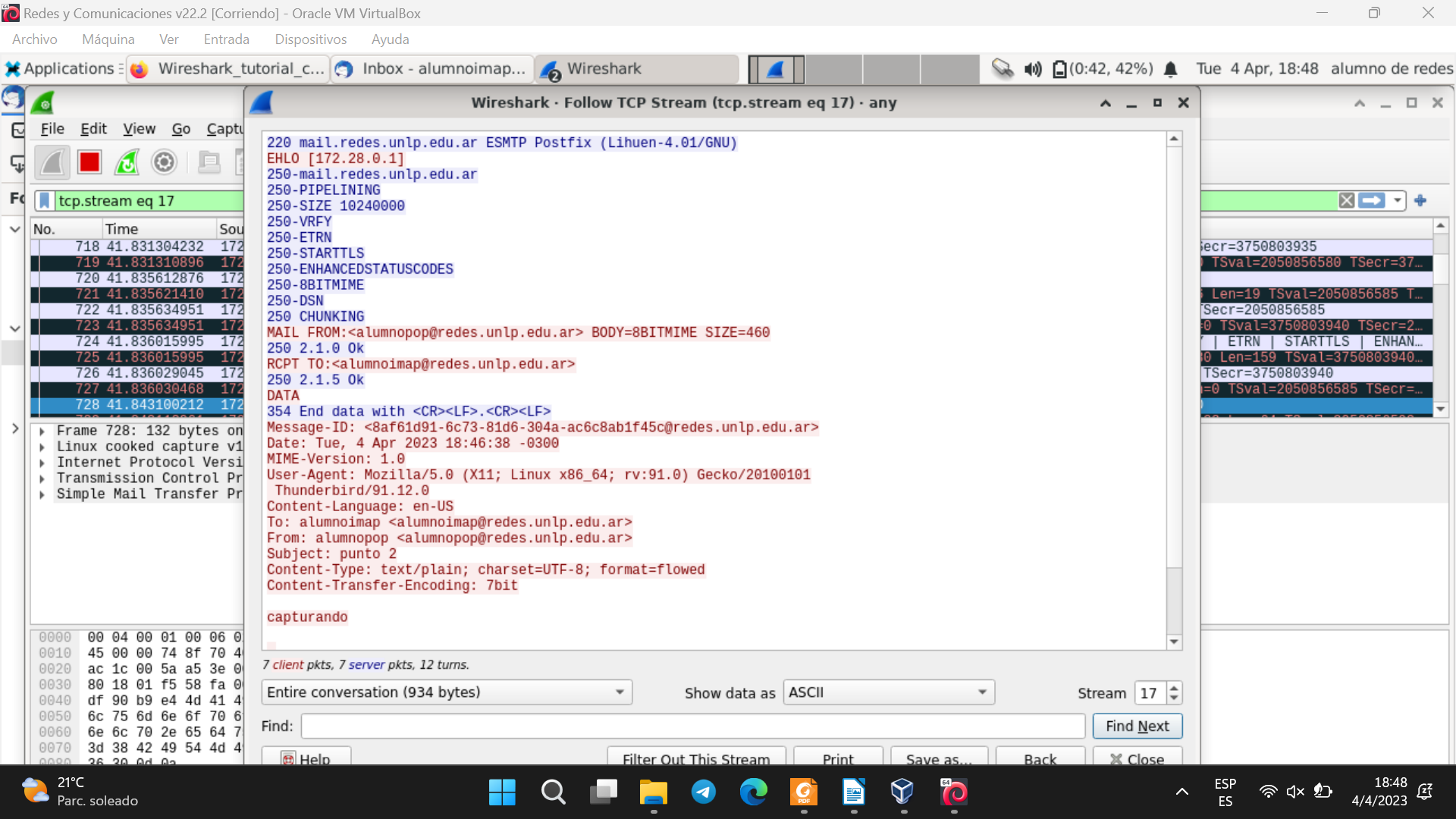
**ii. Utilice el filtro SMTP para observar los paquetes del protocolo SMTP en la captura generada y**

**analice el intercambio de dicho protocolo entre el cliente y el servidor para observar los distintos**

**comandos utilizados y su correspondiente respuesta. Ayuda: filtre por protocolo SMTP y sobre**

**alguna de las líneas del intercambio haga click derecho y seleccione Follow TCP Stream. . .**

****

****

//linea final que no sale en la captura

250 2.0.0 ok: queued as E13C3242395

QUIT

221 2.0.0 Bye

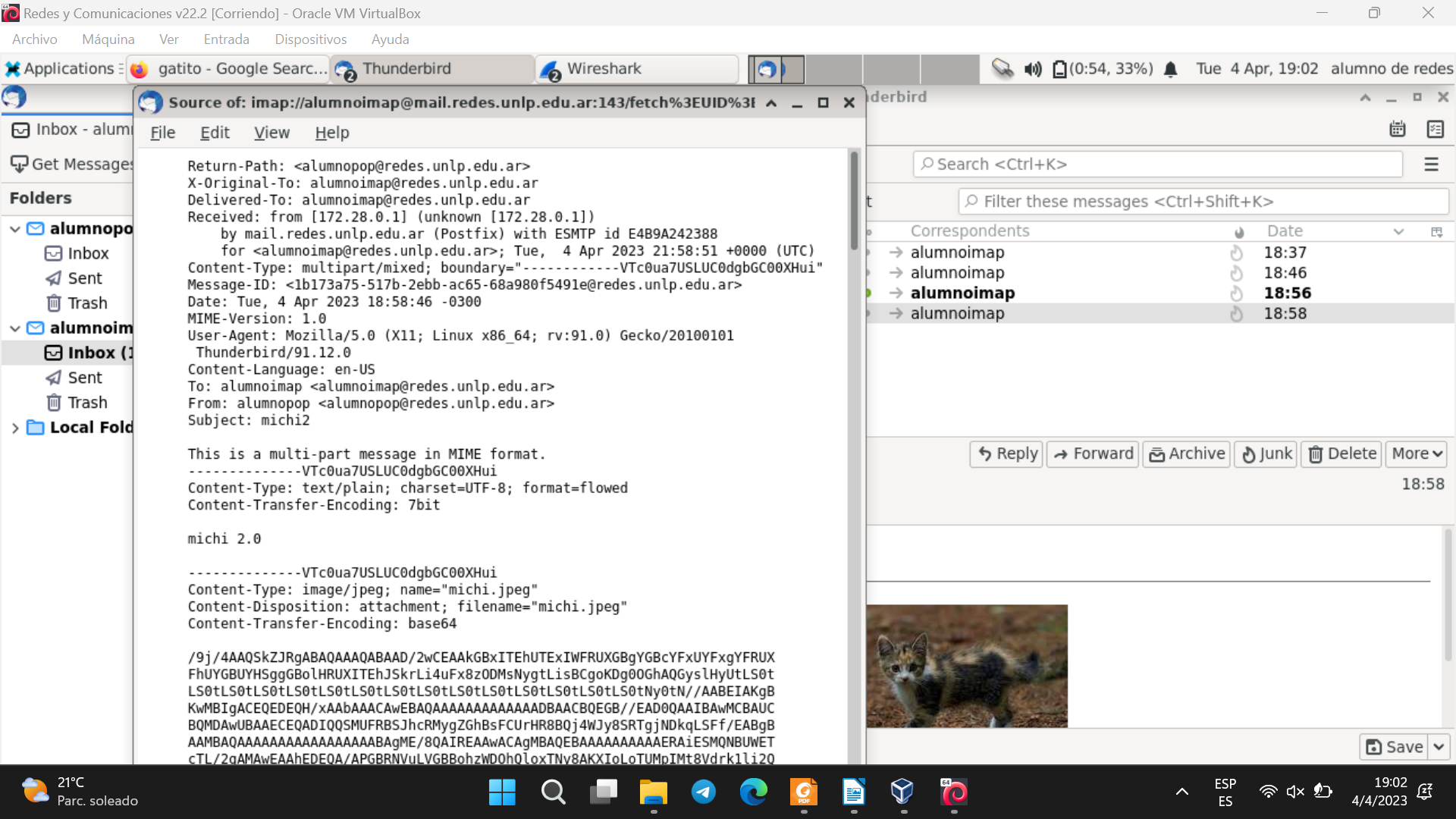
**c. Usando el cliente de correo, thunderbird del usuario alumnopop@redes.unlp.edu.ar envíe un correo**

**electrónico alumnoimap@redes.unlp.edu.ar el cual debe tener: un asunto, datos en el body y una**

**imagen adjunta.**

**i. Verifique los fuentes del correo recibido para entender como se utiliza el header “Content-Type:**

**multipart/mixed“ para poder realizar el envío de distintos archivos adjuntos.**



**ii. Extraiga la imagen adjunta del mismo modo que lo hace el cliente de correo a partir de los**

**fuentes del mensaje.**

Para mandar una imagen se encripta e indica con qué (en este caso base64).

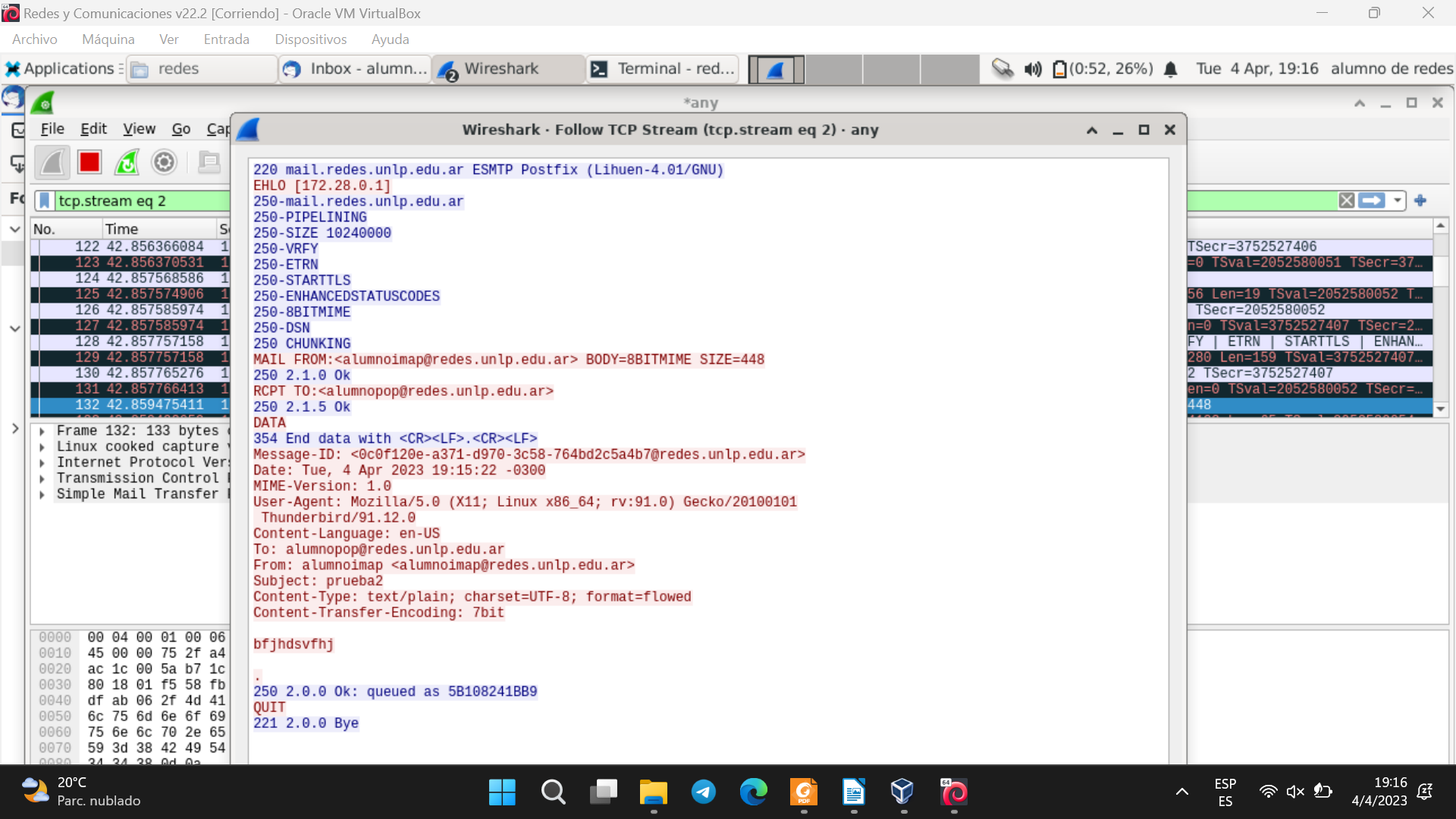
Comando para obtener la imagen: *echo -n “todo lo encriptado” | base64 -d > “path/nombre.extimg”*

**4. Análisis del protocolo POP**

**a. Utilizando Wireshark, capture el tráfico de red contra el servidor de correo mientras desde la cuenta de**

**alumnoimap@redes.unlp.edu.ar le envía una correo a alumnopop@redes.unlp.edu.ar y mientras**

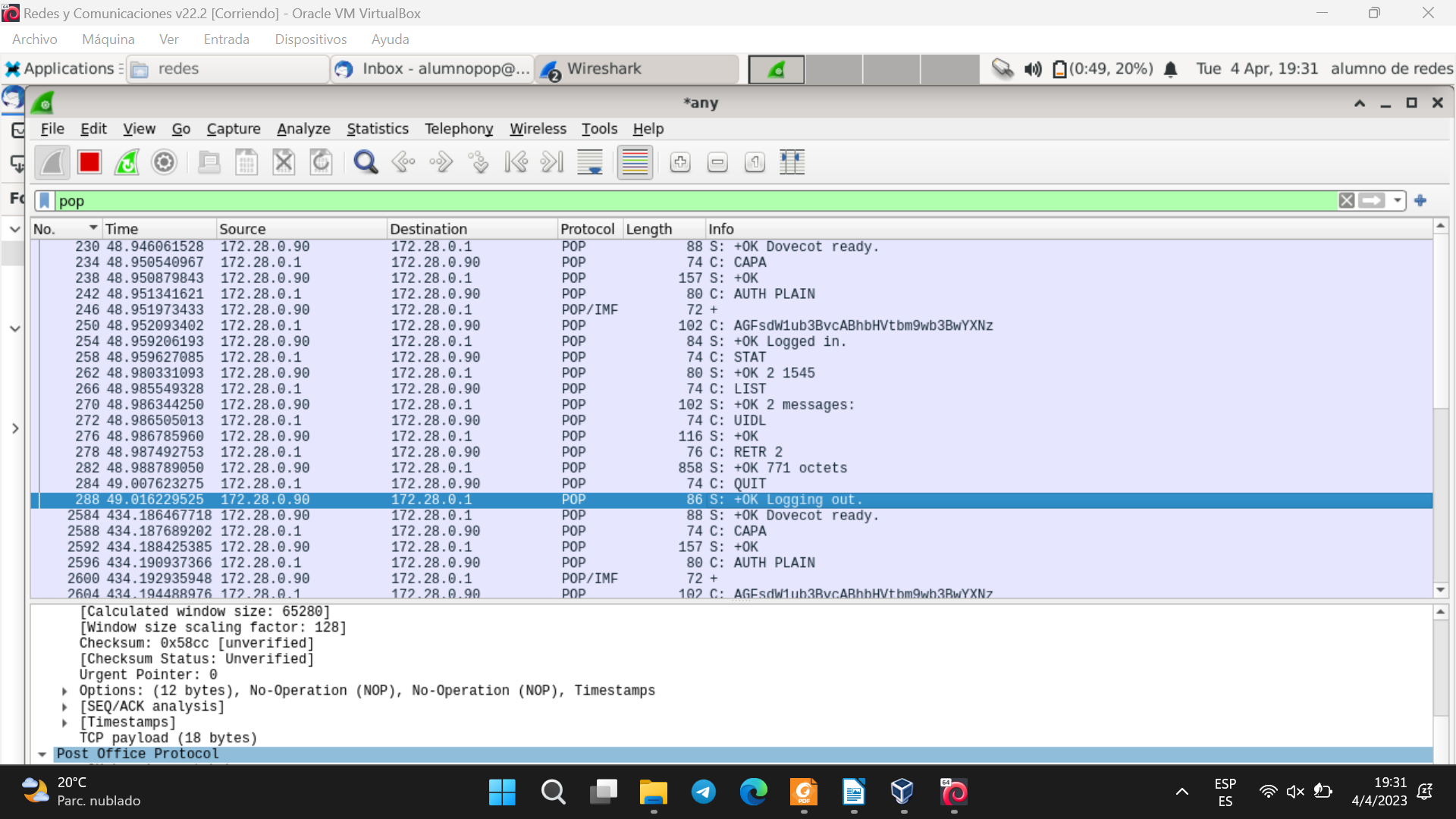
**alumnopop@redes.unlp.edu.ar recepciona dicho correo.**

****

**b. Utilice el filtro POP para observar los paquetes del protocolo POP en la captura generada y analice**

**el intercambio de dicho protocolo entre el cliente y el servidor para observar los distintos comandos**

**utilizados y su correspondiente respuesta.**



**5. Análisis del protocolo IMAP**

**a. Utilizando Wireshark, capture el tráfico de red contra el servidor de correo mientras desde la cuenta**

**alumnopop@redes.unlp.edu.ar le envía un correo a alumnoimap@redes.unlp.edu.ar y mientras**

**alumnoimap@redes.unlp.edu.ar recepciona dicho correo.**

Cuando alumnopop@redes.unlp.edu.ar hace el envío SMTP:

220 mail.redes.unlp.edu.ar ESMTP Postfix (Lihuen-4.01/GNU)

EHLO [172.28.0.1]

250-mail.redes.unlp.edu.ar

250-PIPELINING

250-SIZE 10240000

250-VRFY

250-ETRN

250-STARTTLS

250-ENHANCEDSTATUSCODES

250-8BITMIME

250-DSN

250 CHUNKING

MAIL FROM:<alumnopop@redes.unlp.edu.ar> BODY=8BITMIME SIZE=458

250 2.1.0 Ok

RCPT TO:<alumnoimap@redes.unlp.edu.ar>

250 2.1.5 Ok

DATA

354 End data with <CR><LF>.<CR><LF>

Message-ID: <5184d81f-499d-3c78-1e33-5372ad44a4d4@redes.unlp.edu.ar>

Date: Sat, 17 Sep 2022 18:22:14 -0300

MIME-Version: 1.0

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:91.0) Gecko/20100101

Thunderbird/91.13.0

Content-Language: en-US

To: alumnoimap <alumnoimap@redes.unlp.edu.ar>

From: alumnopop <alumnopop@redes.unlp.edu.ar>

Subject: POP a IMAP

Content-Type: text/plain; charset=UTF-8; format=flowed

Content-Transfer-Encoding: 7bit

Ej 5

.

250 2.0.0 Ok: queued as 886092423ED

QUIT

221 2.0.0 Bye

Cuando alumnoimap@redes.unlp.edu.ar recibe:

\* 7 EXISTS

\* 1 RECENT

DONE

510 OK Idle completed (56.145 + 56.133 + 56.144 secs).

511 noop

511 OK NOOP completed (0.001 + 0.000 secs).

512 UID fetch 9:\* (FLAGS)

\* 7 FETCH (UID 9 FLAGS (\Recent))

512 OK Fetch completed (0.001 + 0.000 secs).

513 UID fetch 9 (UID RFC822.SIZE FLAGS BODY.PEEK[HEADER.FIELDS (From To Cc Bcc Subject Date Message-ID Priority X-Priority References Newsgroups In-Reply-To Content-Type Reply-To)])

\* 7 FETCH (UID 9 RFC822.SIZE 783 FLAGS (\Recent) BODY[HEADER.FIELDS (FROM TO CC BCC SUBJECT DATE MESSAGE-ID PRIORITY X-PRIORITY REFERENCES NEWSGROUPS IN-REPLY-TO CONTENT-TYPE REPLY-TO)] {282}

Message-ID: <5184d81f-499d-3c78-1e33-5372ad44a4d4@redes.unlp.edu.ar>

Date: Sat, 17 Sep 2022 18:22:14 -0300

To: alumnoimap <alumnoimap@redes.unlp.edu.ar>

From: alumnopop <alumnopop@redes.unlp.edu.ar>

Subject: POP a IMAP

Content-Type: text/plain; charset=UTF-8; format=flowed

)

513 OK Fetch completed (0.004 + 0.000 + 0.003 secs).

514 UID fetch 9 (UID RFC822.SIZE BODY.PEEK[])

\* 7 FETCH (UID 9 RFC822.SIZE 783 BODY[] {783}

Return-Path: <alumnopop@redes.unlp.edu.ar>

X-Original-To: alumnoimap@redes.unlp.edu.ar

Delivered-To: alumnoimap@redes.unlp.edu.ar

Received: from [172.28.0.1] (unknown [172.28.0.1])

by mail.redes.unlp.edu.ar (Postfix) with ESMTP id 886092423ED

for <alumnoimap@redes.unlp.edu.ar>; Sat, 17 Sep 2022 21:22:20 +0000 (UTC)

Message-ID: <5184d81f-499d-3c78-1e33-5372ad44a4d4@redes.unlp.edu.ar>

Date: Sat, 17 Sep 2022 18:22:14 -0300

MIME-Version: 1.0

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:91.0) Gecko/20100101

Thunderbird/91.13.0

Content-Language: en-US

To: alumnoimap <alumnoimap@redes.unlp.edu.ar>

From: alumnopop <alumnopop@redes.unlp.edu.ar>

Subject: POP a IMAP

Content-Type: text/plain; charset=UTF-8; format=flowed

Content-Transfer-Encoding: 7bit

Ej 5

)

514 OK Fetch completed (0.001 + 0.000 secs).

515 IDLE

+ idling

DONE

515 OK Idle completed (0.007 + 0.007 + 0.006 secs).

516 uid store 9 +FLAGS (Junk)

\* 7 FETCH (UID 9 FLAGS (\Recent Junk))

516 OK Store completed (0.001 + 0.000 secs).

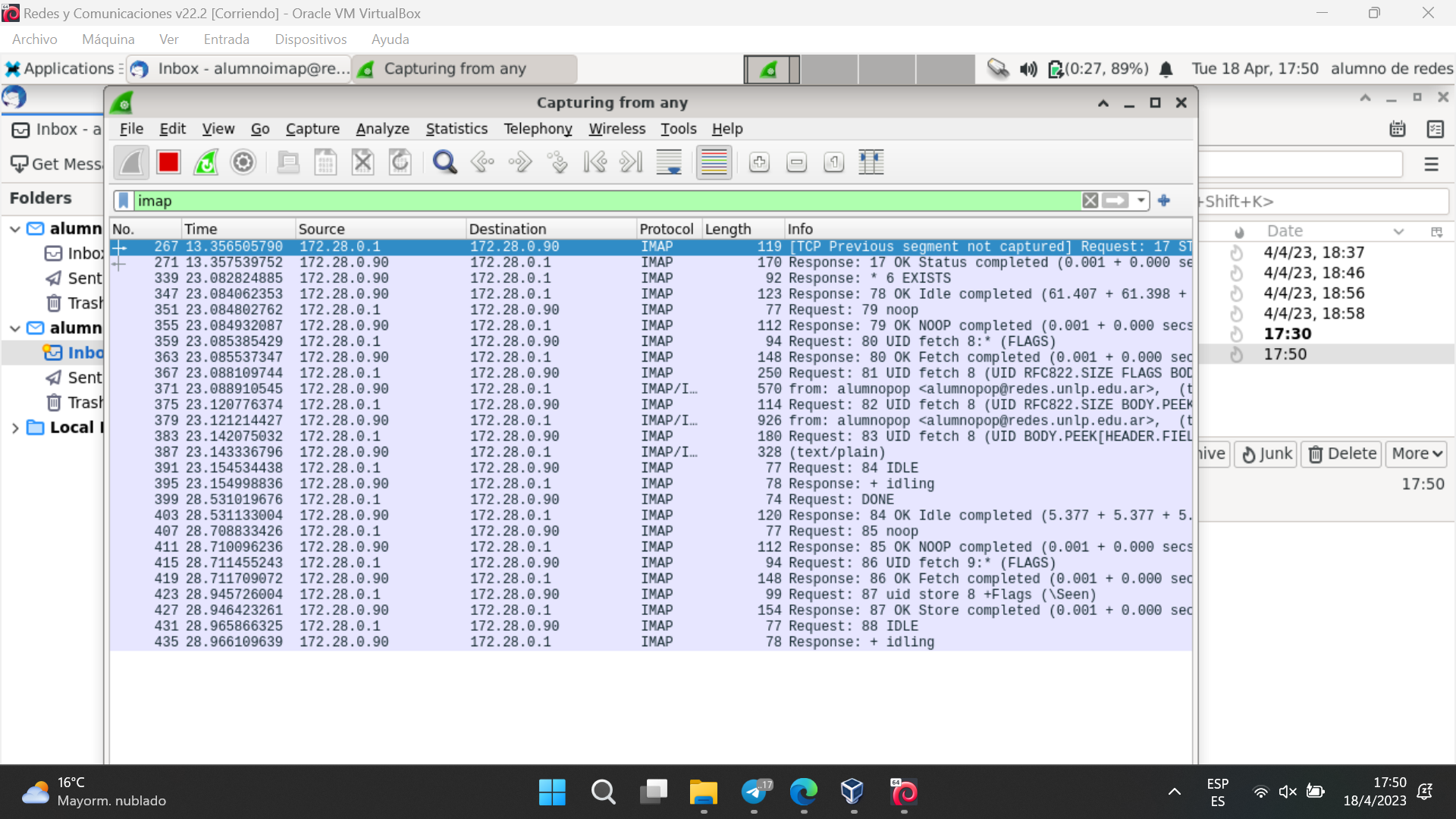
517 IDLE

+ idling

**b. Utilice el filtro IMAP para observar los paquetes del protocolo IMAP en la captura generada y analice**

**el intercambio de dicho protocolo entre el cliente y el servidor para observar los distintos comandos**

**utilizados y su correspondiente respuesta.**

****

**6. IMAP vs POP**

**a. Marque como leídos todos los correos que tenga en el buzón de entrada de alumnopop y de alumnoimap. Luego, cree una carpeta llamada POP en la cuenta de alumnopop y una llamada IMAP en**

**la cuenta de alumnoimap.**

**Asegurese que tiene mails en el inbox y en la carpeta recientemente creada en cada una de las**

**cuentas.**

**b. Cierre la sesión iniciada e ingrese nuevamente identificandose como usuario root y password packer,**

**ejecute el cliente de correos.**

**De esta forma, iniciará el cliente de correo con el perfil del superusuario (diferente del usuario con**

**el que ya configuró las cuentas antes mencionadas).**

**Luego configure las cuentas POP e IMAP de los usuarios alumnopop y alumnoimap como se describió anteriormente pero desde el cliente de correos ejecutado con el usuario root.**

**Luego responda:**

**i. ¿Qué correos ve en el buzón de entrada de ambas cuentas? ¿Están marcados como leídos o**

**como no leídos? ¿Por qué?**

En la cuenta POP3 se ven los correos como no leídos y no se visualizan las carpetas. En cambio, en la cuenta IMAP los correos están como leídos y se visualizan las carpetas personales.

Esto se debe a que IMAP, a diferencia de POP3, mantiene el estado en el servidor. En POP3 el estado es local, y al loguearse con root, hubo un cambio de usuario en el sistema y por ende, no se ven las configuraciones del usuario anterior.

**ii. ¿Qué pasó con las carpetas POP e IMAP que creó en el paso anterior?**

En POP ya no existen. En IMAP sí.

**c. En base a lo observado. ¿Qué protocolo le parece mejor? ¿POP o IMAP? ¿Por qué? ¿Qué protocolo**

**considera que utiliza más recursos del servidor? ¿Por qué?**

En general, se recomienda IMAP.

|  |  |  |
| --- | --- | --- |
|  | **IMAP** | **POP** |
|  | Se accede y administra el correo directamente desde el servidor. | Los mensajes se descargan en la PC y se borran del servidor. |
| Acceso | Puesto que los emails se almacenan en el servidor, puedes acceder a éstos desde varios equipos. | Puesto que los emails se han guardado en tu equipo, solo se puede acceder a ellos desde este. |
| Almacenamiento | Al llegar al límite de almacenamiento online, hay que eliminar mails | No hay problemas con almacenamiento online, los mensajes se guardan en el equipo, el límite es el tamaño del disco. |
| Copia de seguridad | Se hace una copia de seguridad automáticamente. Si por error se elimina un mensaje, se puede recuperar | Es aconsejable instalar un sistema de copia de seguridad en el equipo por si necesitas recuperar emails perdidos o eliminados. |
| Conexión a internet | Sin esta, no se puede acceder a los mails | Necesaria para para descargar los emails, pero posteriormente se pueden ver los mails sin esta. |

IMAP es más complejo y utiliza más recursos del lado del servidor, ya que debe almacenar el estado de los emails en estructuras configurables y además debe procesar una mayor cantidad de comandos y más complejos.

**SMPT enviar, POP e IMAP para recibir**

**7. ¿En algún caso es posible enviar más de un correo durante una misma conexión tcp?**

[**Cómo funciona el correo electrónico (MTA, MDA, MUA) - Blog de Especialistas Hosting**](https://www.especialistashosting.com/blog/2016/12/como-funciona-el-correo-electronico/)

**Considere:**

**MUA = Mail User Agent**

**MSA = Mail Submission Agent**

**MTA = Mail Transfer Agent**

**el nombre del no se puede buscar, lo da el servidor**

LEER LA RFC

**Destinatarios múltiples del mismo dominio entre MUA-MSA y entre MTA-MTA**

**Destinatarios múltiples de diferentes dominios entre MUA-MSA y entre MTA-MTA (este NO porque cada MTA es particular del dominio. Si sale de gmail a yahoo, va a haber una, de gmail a hotmail otra…..)**

**entre servidores MTA se usa MX para conocer el nombre(?) del otro servidor**

**el MUA no resuelve MX**

|  |  |  |
| --- | --- | --- |
|  | **Mismo dominio** | **Distintos dominios** |
| **MUA-MSA** | Se pueden enviar todos en misma conexión TCP | Se pueden enviar todos en misma conexión TCP |
| **MTA-MTA** | Se pueden enviar todos en misma conexión TCP | No se puede, debe hacerse una conexión TCP por cada dominio receptor |

**8. Indique si es posible que el MSA escuche en un puerto TCP diferente a los convencionales y qué**

**implicancias tendría.**

Con el MSA es posible, pero requiere que el MUA esté configurado para hablarle a ese puerto. Esto se puede documentar, si es uno quien debe configurarlo.

**9. Indique si es posible que el MTA escuche en un puerto TCP diferente a los convencionales y qué implicancias tendría.**

Con el MTA, si bien es posible, no es viable. Habría que indicarle a todos los MTAs del mundo que le hablen a ese puerto.

**10. Ejercicio integrador HTTP, DNS y MAIL**

**Suponga que registró bajo su propiedad el dominio redes2022.com.ar y dispone de 4 servidores:**

* **Un servidor DNS instalado configurado como primario de la zona redes2022.com.ar. (hostname: ns1 / ip: 203.0.113.65).**
* **Un servidor DNS instalado configurado como secundario de la zona redes2022.com.ar. (hostname: ns2 / ip: 203.0.113.66).**
* **Un servidor de correo electrónico (hostname: mail / ip: 203.0.113.111). Permitirá a los usuarios enviar y recibir correos a cualquier dominio de Internet.**
* **Un servidor WEB para el acceso a un webmail (hostname: correo / ip: 203.0.113.8). Permitirá a los usuarios gestionar vía web sus correos electrónicos a través de la URL https://webmail.redes2022.com.ar**

**a. ¿Qué información debería informar al momento del registro para hacer visible a Internet el dominio**

**registrado?**

Necesita informar, al servidor con autoridad sobre com.ar.:

i) Que ns1.redes2022.com.ar y ns2.redes2022.com.ar son servidores DNS para el dominio redes2022.com.ar (registros NS)

ii) Que ns1.redes2022.com.ar es el servidor primario para el dominio redes2022.com.ar (registro SOA)

iii) Que las IPv4 de ns1.redes2022.com.ar y ns2.redes2022.com.ar son 203.0.113.65 y 203.0.113.66 respectivamente (registros A)

**b. ¿Qué registros sería necesario configurar en el servidor de nombres? Indique toda la información**

**necesaria del archivo de zona. Puede utilizar la siguiente tabla de referencia (evalúe la necesidad de**

**usar cada caso los siguientes campos): Nombre del registro, Tipo de registro, Prioridad, TTL, Valor**

**del registro.**

|  |
| --- |
| redes2022.com.ar. 86400 IN SOA ns1.redes2022.com.ar. email\.admin.redes2022.com.ar. 2022091700 604800 86400 2419200 86400  redes2022.com.ar. 86400 IN NS ns1.redes2022.com.ar. redes2022.com.ar. 86400 IN NS ns2.redes2022.com.ar. redes.unlp.edu.ar. 86400 IN MX 5 mail.redes2022.com.ar.  mail.redes2022.com.ar. 86400 IN A 203.0.113.111  webmail.redes2022.com.ar. 604800 IN A 203.0.113.8 ns1.redes2022.com.ar. 604800 IN A 203.0.113.65 ns2.redes2022.com.ar. 604800 IN A 203.0.113.66  redes2022.com.ar. 86400 IN SOA ns1.redes2022.com.ar. email\.admin.redes2022.com.ar. 2022091700 604800 86400 2419200 86400 |

**c. ¿Es necesario que el servidor de DNS acepte consultas recursivas? Justifique.**

No, porque al ser el que tiene autoridad sobre la zona, es capaz de devolver las IPs de los dominios solicitados. No es su responsabilidad poder resolver otros dominios externos (aunque podés configurarlo para que lo haga).

**d. ¿Qué servicios/protocolos de capa de aplicación configuraría en cada servidor?**

i) ns1: DNS

ii) ns2: DNS

iii) mail: SMTP, POP/IMAP

iv) correo: HTTP(S), recordar que correo es un hostname (osea no es algo relevante)

(Consultar porque “correo” es en realidad un servidor web para acceder a un webmail)

**e. Para cada servidor, ¿qué puertos considera necesarios dejar abiertos a Internet? A modo de referencia, para cada puerto indique: servidor, protocolo de transporte y número de puerto.**

|  |  |  |
| --- | --- | --- |
| **Servidor** | **Protocolo de transporte** | **Número de puerto** |
| ns1 | UDP, TCP | 53 (DNS) |
| ns2 | UDP, TCP | 53 (DNS) |
| mail | TCP | 25, 110, 995, 143, 993 (SMTP, POP, POP, IMAP, IMAP). Ver si es solo smtp -envía- o pop e imap tamb (recibe) |
| correo | TCP | 80, 443 (HTTP, HTTPS) |

**Ver que al googlear dice que DNS usa udp y tcp -> usan el mismo número de puerto**

**f. ¿Cómo cree que se conectaría el webmail del servidor web con el servidor de correo? ¿Qué protocolos usaría y para qué?**

El WebMail recibiría solicitudes HTTP, y para satisfacerlas se comunicaría con el servidor de correo, usando:

i) SMTP: Enviar emails a otros usuarios (Protocolo para transferencia simple de mails)

ii) IMAP: Almacenar y recibir emails, gestionar carpetas, etc

**g. ¿Cómo se podría hacer para que cualquier MTA reconozca como válidos los mails provenientes del**

**dominio redes2022.com.ar solamente a los que llegan de la dirección 203.0.113.111? ¿Afectaría**

**esto a los mails enviados desde el Webmail? Justifique.**

i) SPF (Sender Policy Framework), no tanto PTR (Pointer records) (Quiere decir que es mas importante registrar el mail en el SPF que utilizar los PTR?)

SPF es un protocolo de autenticación de correo electrónico que permite que se especifique a quién se permite enviar correo electrónico en nombre de su dominio. Se puede autorizar a los remitentes para los proveedores de correo electrónico en el sistema de nombres de dominio (DNS). Ese **registro SPF** incluye una lista de las direcciones IP aprobadas y de las direcciones IP de los proveedores.

Antes de entregar un mensaje, los proveedores de correo electrónico verifican el registro SPF, para lo cual buscan el dominio que se incluye en la dirección de “remitente de sobre” (que también se conoce como ruta de devolución o “mfrom”) en el encabezado técnico oculto del mensaje. Si la dirección IP que envía el mensaje en nombre de este dominio no está en la lista de dominios del registro SPF, el mensaje no pasa la autenticación SPF.

Para implementar SPF en el dominio específico, se debería crear un registro SPF en el servidor DNS del dominio. Este registro indica a los servidores de correo electrónico autorizados para enviar correos electrónicos desde el dominio, y también puede especificar las direcciones IP permitidas para enviar correos electrónicos en nombre del dominio.

Cuando un servidor de mail reciba un correo que aparenta ser enviado desde el dominio en cuestión, verificará el registro SPF y comprobará si el remitente se encuentra autorizado y su dirección IP es la indicada. Si la verificación de SPF falla, es probable que el correo electrónico sea considerado como spam o rechazado.

<https://www.hoswedaje.com/seguridad/registros-ptr-que-significan-y-para-que-sirven/>

ii) No afectaría, porque el Webmail le envía los datos al servidor SMTP, y es éste quien emite realmente los emails (nop?)

**h. ¿Qué característica propia de SMTP, IMAP y POP hace que al adjuntar una imagen o un ejecutable**

**sea necesario aplicar un encoding (ej. base64)?**

La característica es que funcionan sobre ASCII de 7 bits (Texto plano). Como los bytes de los archivos pueden tomar cualquier valor (incluyendo caracteres no válidos), al codificarlos se restringe el conjunto de valores a caracteres ASCII válidos

**i. ¿Se podría enviar un mail a un usuario de modo que el receptor vea que el remitente es un usuario**

**distinto? En caso afirmativo, ¿Cómo? ¿Es una indicación de una estafa? Justifique**

i) Sería posible, modificando el valor del encabezado From:

ii) Suena a estafa -.-

**j. ¿Se podría enviar un mail a un usuario de modo que el receptor vea que el destinatario es un usuario**

**distinto? En caso afirmativo, ¿Cómo? ¿Por qué no le llegaría al destinatario que el receptor vé? ¿Es**

**esto una indicación de una estafa? Justifique**

i) Sería posible, modificando el valor del encabezado To:

ii) No le llegaría ya que el destinatario se indica al servidor SMTP mediante comandos, y no se toma de lo escrito en los headers del mail

iii) Para mí no sería una estafa, aunque para un usuario sí que sería raro ver algo así. También depende del contenido del mensaje

Es importante señalar que la manipulación del campo "To" del encabezado del correo electrónico podría ser detectada y considerada como un intento de suplantación de identidad, lo cual es ilegal y puede tener consecuencias graves.

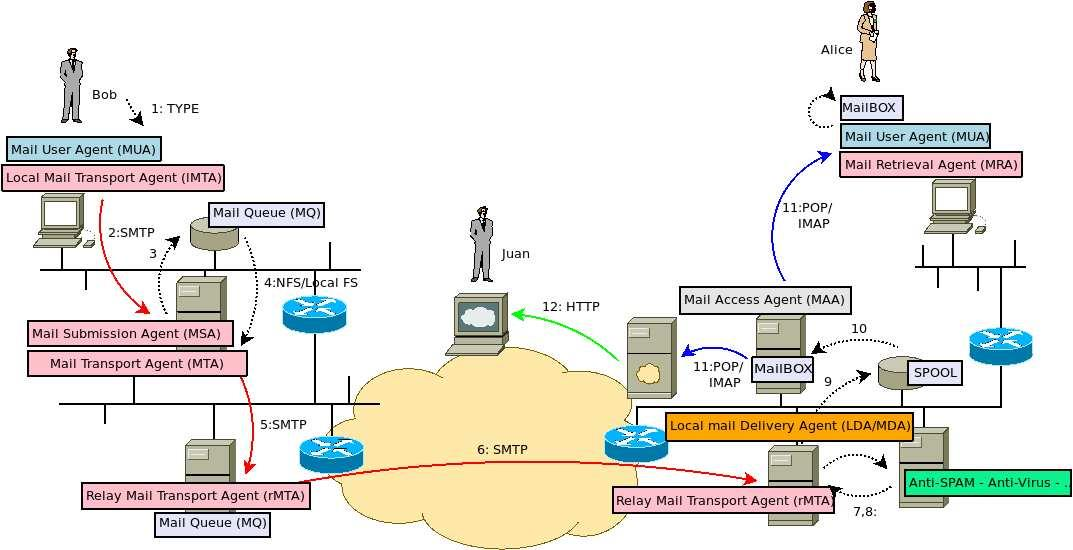
**k. ¿Qué protocolo usará nuestro MUA para enviar un correo con remitente redes@info.unlp.edu.ar?**

**¿Con quién se conectará? ¿Qué información será necesaria y cómo la obtendría?**

i) Usará SMTP para todo lo relacionado a emails, y DNS para obtener direcciones IP

ii) La secuencia simplificada sería, asumiendo indirecciones:

1. El MUA obtiene del DNS la IP del MSA, y se comunica con éste para enviarle los datos del correo
2. El MSA obtiene del DNS la IP del rMTA fuente, y se comunica con éste para enviarle los datos del correo
3. El rMTA fuente extrae de la dirección de correo destino, el nombre del dominio destino
4. El rMTA fuente obtiene del DNS la IP del rMTA destino, y se comunica con éste para enviarle los datos del correo



**l. Dado que solo disponemos de un servidor de correo, ¿qué sucederá con los mails que intenten**

**ingresar durante un reinicio del servidor?**

l) El reinicio interrumpirá la comunicación SMTP (o no llega a iniciarse). Entonces, el servidor fuente detectará esto y guardará el email en una cola interna, reintentando periódicamente enviar el correo. Si no puede enviarlo, se rendirá e informará esto al usuario.

Si no está disponible va a haber timeout o el TCP va a responder un RST ACK, en ese caso, si hay un registro MX secundario se va a enviar ahí, sino, como dice arriba, espera a ver si lo logra reenviar durante x tiempo.

Es TCP

**m. Suponga que contratamos un servidor de correo electrónico en la nube para integrarlo con nuestra**

**arquitectura de servicios.**

**i. ¿Cómo configuraría el DNS para que ambos servidores de correo se comporten de manera de**

**dar un servicio de correo tolerante a fallos?**

m) Habría que agregar, al archivo de zona:

redes.unlp.edu.ar. 86400 IN MX 10 nube.redes2022.com.ar.

nube.redes2022.com.ar. 86400 IN A 203.0.113.112 **🡪Que es esa A?**

**11. Utilizando la herramienta Swaks envíe un correo electrónico con las siguientes características:**

**Dirección destino: Dirección de correo de alumnoimap@redes.unlp.edu.ar**

**Dirección origen: redesycomunicaciones@redes.unlp.edu.ar**

**Asunto: SMTP-Práctica4**

**Archivo adjunto: PDF del enunciado de la práctica**

**Cuerpo del mensaje: Esto es una prueba del protocolo SMTP**

**a. Analice tanto la salida del comando swaks como las fuentes del mensaje recibido para responder**

**las siguientes preguntas:**

**i. ¿A qué corresponde la información enviada por el servidor destino como respuesta al comando**

**EHLO? Elija dos de las opciones del listado e investigue la funcionalidad de la misma.**

Indica las funcionalidades soportadas por el servidor SMTP

STARTTLS: El servidor soporta TLS, para encriptar la comunicación con el cliente

PIPELINING: El servidor soporta recibir múltiples comandos por conexión TCP, lo cual mejora la eficiencia

**ii. Indicar cuáles cabeceras fueron agregadas por la herramienta swaks.**

Swaks agregó:

(1) Date: Mon, 19 Sep 2022 14:45:04 -0300

(2) Message-Id: <20220919144504.020342@debian>

(3) X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/

(4) MIME-Version: 1.0

(5) Content-Type: multipart/mixed; boundary="----=\_MIME\_BOUNDARY\_000\_20342"

(6) ------=\_MIME\_BOUNDARY\_000\_20342

(7) Content-Type: text/plain

(8) ------=\_MIME\_BOUNDARY\_000\_20342

(9) Content-Type: application/octet-stream; name="@p04.pdf"

(10) Content-Description: @p04.pdf

(11) Content-Disposition: attachment; filename="@p04.pdf"

(12) Content-Transfer-Encoding: BASE64

**iii. ¿Cuál es el message-id del correo enviado? ¿Quién asigna dicho valor?**

(1) La ID es 20220919144504.020342@debian

(2) Este valor es asignado por el cliente de correos

**iv. ¿Cuál es el software utilizado como servidor de correo electrónico?**

iv) El software es swaks v20201014.0

**v. Adjunte la salida del comando swaks y los fuentes del correo electrónico.**

v) Veanse los dos archivos txt en:[**https://drive.google.com/drive/folders/1ImQx8OHi8iddFeA04ZMpag-XwsrbpIN5**](https://drive.google.com/drive/folders/1ImQx8OHi8iddFeA04ZMpag-XwsrbpIN5)

**b. Descargue de la plataforma la captura de tráfico smtp.pcang y la salida del comando swaks smtp.swaks para responder y justificar los siguientes ejercicios.**

**i. ¿Por qué el contenido del mail no puede ser leido en la captura de tráfico?**

No pudo ser leído, porque el servidor y cliente empezaron a comunicarse a través de TLS. Como encripta el contenido, desde Wireshark si no se tiene la clave usada, no es posible desencriptarlo

**c. Realice una consulta de DNS por registros TXT al dominio info.unlp.edu.ar y entre dichos registros**

**evalúe la información del registro SPF. ¿Por qué cree que aparecen muchos servidores autorizados?**

dig "info.unlp.edu.ar" txt

; <<>> DiG 9.16.1-Ubuntu <<>> info.unlp.edu.ar txt

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47030

;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 65494

;; QUESTION SECTION:

;info.unlp.edu.ar. IN TXT

;; ANSWER SECTION:

info.unlp.edu.ar. 300 IN TXT "google-site-verification=S5DXBH0Y\_JiAEZ0VYUsukCNH35qBwL7KV1jwzZawRsE"

info.unlp.edu.ar. 300 IN TXT "MS=53F37089CAA39175A9111FF830E7F978A6B8036E"

info.unlp.edu.ar. 300 IN TXT "v=spf1 mx a:mail3.info.unlp.edu.ar a:listas.extension.info.unlp.edu.ar a:mail-app.info.unlp.edu.ar

a:biblioteca.info.unlp.edu.ar a:catedras.info.unlp.edu.ar a:moodle.linti.unlp.edu.ar ~all"

info.unlp.edu.ar. 300 IN TXT "google-site-verification=\_KuE\_Fg0H37zv4e7OVJVyl\_qGpamol5t\_pMisXadMRU"

info.unlp.edu.ar. 300 IN TXT "google-site-verification=GQLud3qGeuqjRPOn-2INvgU0D-dkJUjvGrXICDqACgQ"

;; Query time: 56 msec

;; SERVER: 127.0.0.53#53(127.0.0.53)

;; WHEN: lun sep 19 03:48:48 -03 2022

;; MSG SIZE rcvd: 545

i) Esto es así porque existen múltiples servidores de emails autorizados para enviar correos, que son parte de la Facultad de Informática

**d. Realice una consulta de DNS por registros TXT al dominio outlook.com y analice el registro correspondiente a SPF. ¿Cuáles son los bloques de red autorizados para enviar mails?. Investigue para qué se utiliza la directiva "~all"**

*dig "outlook.com" txt*

; <<>> DiG 9.16.1-Ubuntu <<>> outlook.com txt

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9206

;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 65494

;; QUESTION SECTION:

;outlook.com. IN TXT

;; ANSWER SECTION:

outlook.com. 300 IN TXT "google-site-verification=DC2uC-T8kD33lINhNzfo0bNBrw-vrCXs5BPF5BXY56g"

outlook.com. 300 IN TXT "google-site-verification=0iLWhIMhXEkeWwWfFU4ursTn-\_OvoOjaA0Lr7Pg1sEM"

outlook.com. 300 IN TXT "v=spf1 include:spf-a.outlook.com include:spf-b.outlook.com ip4:157.55.9.128/25 include:spf.protection.outlook.com include:spf-a.hotmail.com include:\_spf-ssg-b.mic

rosoft.com include:\_spf-ssg-c.microsoft.com ~all"

;; Query time: 48 msec

;; SERVER: 127.0.0.53#53(127.0.0.53)

;; WHEN: lun sep 19 03:50:26 -03 2022

;; MSG SIZE rcvd: 425

i) Los bloques son:

(1) spf-a.outlook.com

(2) spf-b.outlook.com

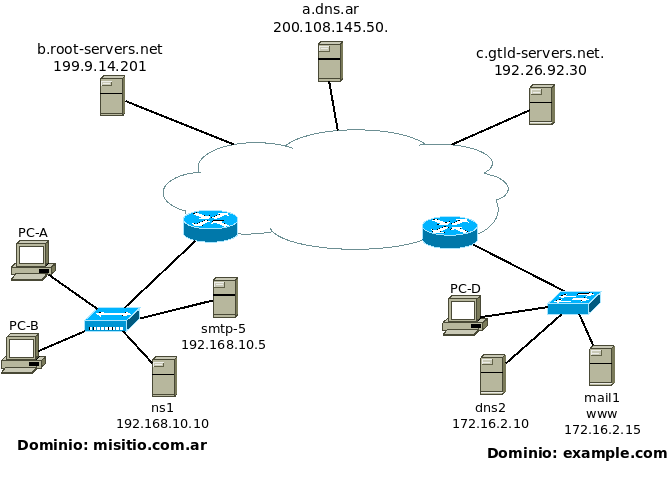
(3) spf.protection.outlook.com

(4) spf-a.hotmail.com

(5) \_spf-ssg-b.mic

ii) El ~all se usa para especificar que, si un servidor de correo o dirección IP no se encuentran en el listado del registro SPF, deberán ser aceptados agregándoles una marca de posible spam

**12. Observar el gráfico a continuación y teniendo en cuenta lo siguiente, responder:**



**El usuario** [**juan@misitio.com.ar**](mailto:juan@misitio.com.ar) **en PC-A desea enviar un mail al usuario** [**alicia@example.com**](mailto:alicia@example.com)**. Cada organización tiene sus propios servidores de DNS y Mail**

**El servidor ns1 de misitio.com.ar no tiene la recursión habilitada**

**a. El servidor de mail, mail1, y de HTTP, www, de example.com tienen la misma IP, ¿es posible esto?**

**Si lo es, ¿cómo lo resolvería?**

Es posible, porque los servicios HTTP y SMTP usan distintos puertos para funcionar, aunque sean hosteados en una misma máquina física

**b. Al enviar el mail, ¿por qué registro de DNS consultará el MUA?**

Consultará por los registros MX del dominio misitio.com.ar., y luego, el registro A de smtp-5.misitio.com.ar. (si en la respuesta al MX no se incluyó su IP como información adicional)

**c. Una vez que el mail fue recibido por el servidor smtp-5, ¿por qué registro de DNS consultará?**

Consultará por los registros MX del dominio example.com., y luego, el registro A de mail1.example.com. (si en la respuesta al MX no se incluyó su IP como información adicional)

Orden: registro MX propio, si no vino la IP incluida, se consulta por la IP (registro A)

Cuando el mail lo recibe el servidor ismp, este consulta por el mx destino y, si no recibe su ip, por el registro A.

**d. Si en el punto anterior smtp-5 recibiese un listado de nombres de servidores de correo, ¿será necesario realizar una consulta de DNS adicional? Si es afirmativo, ¿por qué tipo de registro y de cuál servidor preguntaría?**

Si en la respuesta al MX no se incluyeron las IPs como información adicional, entonces se consultaría por el registro A de cada servidor SMTP en función de su prioridad (orden ascendente). Si el primero falla, se consulta al segundo, y así sucesivamente

**e. Indicar todo el proceso que deberá realizar el servidor ns1 de misitio.com.ar para obtener los servidores de mail de example.com**

**Primero debe averiguar a que IP corresponde example.com si no la tiene, despues debe consultar en esa ip para conseguir un listado de los servidores de mail (que facil, no?)**

**f. Teniendo en cuenta el proceso de encapsulación/desencapsulación y definición de protocolos, responder V o F y justificar:**

**Los datos de la cabecera de SMTP deben ser analizados por el servidor DNS para responder a la consulta de los registros MX**

Falso, porque el servidor SMTP es quien extrae el nombre de dominio a partir de los datos de la cabecera, y luego consulta al servidor DNS por los registros MX

**Al ser recibidos por el servidor smtp-5 los datos agregados por el protocolo SMTP serán analizados por cada una de las capas inferiores**

Falso, porque los datos agregados en la capa de aplicación (SMTP) son recibidos por otra instancia de esa misma capa

**Cada protocolo de la capa de aplicación agregará una cabecera con información propia de ese protocolo**

Verdadero, porque agrega los datos que necesita para poder funcionar

**Como son todos protocolos de la capa de aplicación, las cabeceras agregadas por el protocolo de DNS pueden ser analizadas y comprendidas por el protocolo SMTP o HTTP**

Falso, porque a pesar de pertenecer a la misma capa, se trata de protocolos diferentes entre sí

**Para que los clientes en misitio.com.ar puedan acceder el servidor HTTP** [**www.example.com**](http://www.example.com/) **y mostrar correctamente su contenido deben tener el mismo sistema operativo.**

Falso, porque si todos los sistemas operativos (y navegadores usados, etc) implementan correctamente el protocolo HTTP, usar uno u otro será indistinto

**g. Un cliente web que desea acceder al servidor www.example.com y que no pertenece a ninguno**

**de estos dos dominios puede usar a ns1 de misitio.com.ar como servidor de DNS para resolver la**

**consulta.**

Falso, porque el servidor ns1 tiene la recursión deshabilitada

**h. Cuando Alicia quiera ver sus mails desde PC-D, ¿qué registro de DNS deberá consultarse?**

Consultará por los registros MX del dominio example.com., y luego, el registro A de mail1.example.com. (si en la respuesta al MX no se incluyó su IP como información adicional)

**i. Indicar todos los protocolos de mail involucrados, puerto y si usan TCP o UDP, en el envío y recepción de dicho mail**

|  |  |  |  |
| --- | --- | --- | --- |
| **Protocolo de emails** | **Protocolo de transporte** | **Número de puerto** | **Dirección de los datos** |
| SMTP | TCP | 25 | Envío/Recepción |
| IMAP | TCP | 143 | Envío/Recepción |
| POP | TCP | 110 | Recepción |