Práctica 4

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

   Para él envió de mails entre cliente y servidor se utiliza SMTP. Entre servidores de correo también se utiliza el protocolo SMTP

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

   Para la recepción de correos electrónicos, existen dos protocolos principales: POP3 (Post Office Protocol versión 3) e IMAP (Internet Message Access Protocol).

   POP3 (Post Office Protocol versión 3):

   - **Simplicidad:** POP3 es un protocolo de acceso a correo extremadamente simple. Su simplicidad lo hace fácil de implementar y utilizar.

   - **Descarga y Borrado:** POP3 generalmente se configura para descargar los correos electrónicos desde el servidor a la máquina local del usuario. En este modo, los correos se eliminan del servidor después de la descarga (aunque se pueden configurar para mantener una copia en el servidor).

   - **No Mantiene Estado:** POP3 no mantiene información de estado entre sesiones. Esto significa que no guarda información sobre carpetas, mensajes marcados o cualquier otra información relacionada con el estado de la cuenta del usuario en el servidor.

   - **Limitado para Usuarios Nómadas:** Para usuarios que desean acceder a sus correos electrónicos desde múltiples dispositivos, POP3 puede ser limitante ya que no ofrece una forma sencilla de sincronizar carpetas y correos entre dispositivos.

   IMAP (Internet Message Access Protocol):

   - **Funcionalidad Avanzada:** IMAP es más avanzado que POP3 y ofrece una amplia gama de funcionalidades. Permite a los usuarios organizar correos electrónicos en carpetas remotas, buscar mensajes, mover mensajes entre carpetas y realizar otras acciones avanzadas.

   - **Mantiene Estado:** IMAP mantiene información de estado en el servidor. Esto significa que las carpetas, los mensajes marcados como leídos/no leídos, y otras acciones realizadas en un dispositivo se reflejan en todos los dispositivos conectados, lo que lo hace ideal para usuarios nómadas.

   - **Acceso a Partes Componentes de los Mensajes:** IMAP permite a los usuarios acceder a partes específicas de los mensajes, como la cabecera o

partes de un mensaje MIME. Esto es útil cuando se necesita descargar solo partes específicas de un mensaje para ahorrar ancho de banda.

- **Complejidad Adicional:** Debido a su mayor funcionalidad, IMAP puede ser más complejo de implementar tanto en el lado del cliente como en el lado del servidor en comparación con POP3.

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.**

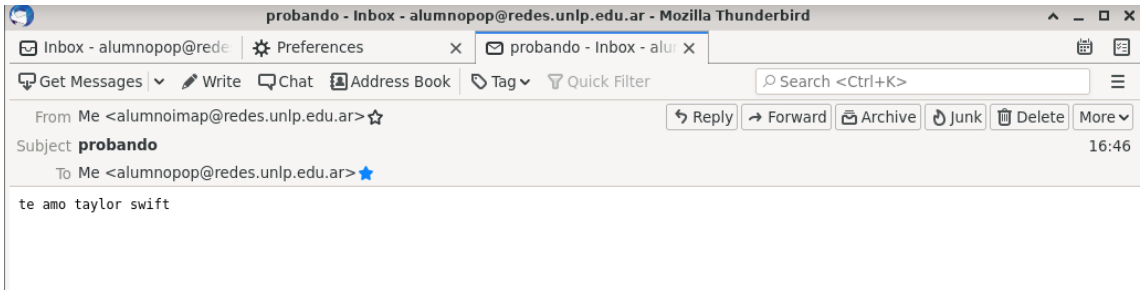
   Al crear cada una de las cuentas, seleccionar Manual config y luego de configurar las mismas según lo indicado, ignorar advertencias por uso de conexión sin cifrado

   <u>Datos para POP</u>
   - **Cuenta de correo: alumnopop@redes.unlp.edu.ar**
   - **Nombre de usuario: alumnopop**
   - **Contraseña: alumnopoppass**
   - **Puerto: 110**

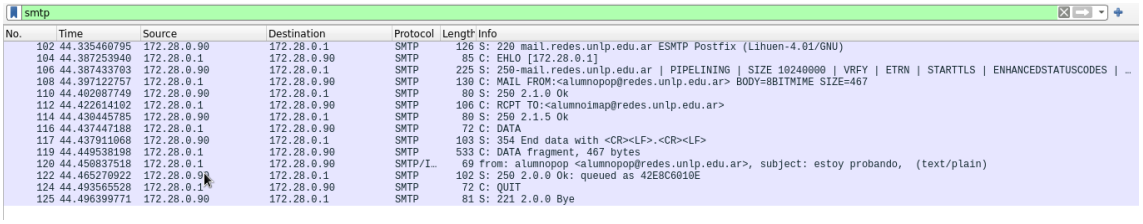
   <u>Datos para IMAP</u>
   - **Cuenta de correo: alumnoimap@redes.unlp.edu.ar**
   - **Nombre de usuario: alumnoimap**
   - **Contraseña: alumnoimappass**
   - **Puerto: 143**

   <u>Datos comunes para ambas cuentas</u>
   - **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**
     - **SSL: None**
     - **Autenticación: Normal password**

   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. . .**




```
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=467
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: <2a0fd16a-fc14-92f0-18fb-4357ceb90e9a@redes.unlp.edu.ar>
Date: Tue, 12 Sep 2023 16:50:13 -0300
MIME-Version: 1.0
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
 Thunderbird/91.12.0
Content-Language: en-US
To: alumnoimap@redes.unlp.edu.ar
From: alumnopop <alumnopop@redes.unlp.edu.ar>
Subject: estoy probando
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit

estoy probando holitas

.
250 2.0.0 Ok: queued as 42E8C6010E
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.**

```
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 12B1C60114
    for <alumnoimap@redes.unlp.edu.ar>; Tue, 12 Sep 2023 19:57:42 +0000 (
Content-Type: multipart/mixed; boundary="------------px0JXq3DNsdR43veRZqH
Message-ID: <647dcd3a-99d1-63ac-66f1-40bb2b467961@redes.unlp.edu.ar>
Date: Tue, 12 Sep 2023 16:57:36 -0300
MIME-Version: 1.0
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
 Thunderbird/91.12.0
Content-Language: en-US
To: alumnoimap@redes.unlp.edu.ar
From: alumnopop <alumnopop@redes.unlp.edu.ar>
Subject: El mejor album de lana del rey

This is a multi-part message in MIME format.
--------------px0JXq3DNsdR43veRZqHptHO
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit

Es nfr

--------------px0JXq3DNsdR43veRZqHptHO
Content-Type: image/jpeg; name="pruebas.jpeg"
Content-Disposition: attachment; filename="pruebas.jpeg"
Content-Transfer-Encoding: base64
```


```
/9j/4AAQSkZJRgABAQAAAQABAAD/2wCEAAoHCBUVFBcUFRUYGBcZGxocGhoaGRwgGhsZGh0a
GhkcHSEiICwkHBwoIBkZJDUkKC0vMjIyGiI4PTgxPCwxMi8BCwsLDw4PHRERHTEoIygxMTEx
MTExMTExMTExMTExMTMxMTEzMTExMzExMTExMTExMTExMTExMTExMTExMTExMf/AABEIARoA
swMBIgACEQEDEQH/xAAcAAACAgMBAQAAAAAAAAAAAAAAFBgMEAAECBwj/xABFEAACAQIDBAcF
BQcACgMBAAABAhEAAwQSIQUxQVEGEyIyYXGBQpGhsfAUI1LB0QdicoKS4fEzQ1Nzk6Kys8LS
JDSDFf/EABkBAAMBAQEAAAAAAAAAAAAAAAIDBAEABf/EADARAAICAQMDAwIFAwUAAAAAAAAB
AhEDEiExBEFRE2FxIqEUgZGGx8DLR4RUzQlLB/9oADAMBAAIRAxEAPwBg6/IAZAMDix9+6sTF
XN+aV/EoUx6mY9aDLtG0ey7FDOX7zsgndpnAnwg61bCG2c1uYI1AMA+R/PhTVT4JHa5Ke3bN
xbiXbdwy4yMrGEYiWTMBu9tc3MpvGlXdnpbuJmEyCMysYKN+FgOInxB3gkQaVr20L2NvC3Yf
```

```
61WV4WQQ19aUcZ0kEWV17bEXOkJJ1Dec/wB6zWglBjo2O17WDD41o3dGGa2J5qDqPKkm/tG2
4hiY/iYH3j9aE4pWtjPYv3Ad+UufgZ+fvrlKztNDZtrbKWiDes51OiuSJ8p7wobtDpBbSEt4
cKxAOZ1GgIkEAzOnGkV7jOxZ2LNxJJJ+Nel2dkjG7Ow92CbtpSunedbbFCuvGFBE8QOZolFX
uZdHlmPSLtzf3ifGT2vzo/0P2c1+/bViWQfeuCSRkQwi/wAz7xyWqnSPZ5S8mU5luqMjcDGj
acIkE+dMPQ7bOFw9u4zMxu3XhbdtGZ+rtjLbXQRJ7R38a2RsG0m/yLt5bmM2mrrIsYRoz8Dc
GrhTxJYBTHBPHVf6d7aF26EtkMiCAY0J1kjzPHkoPGmDGdIEdxh7q3LKmB1FpZuvn1AuMpAt
qQZNtCWMiSNQavTXYGHtWhcSVYmMpYtIgmdZO+BvjtVh0KdruefdaPwj4/rWVjRWUYoYr+Lb
K1uTlDsQOAJJny/zXWHu9gQec/GqWK7zfxN8zW7bQQYnTnU8laLoOmOGzbBuONdIBMgabuPj
T/hGCqOFLOycMLaKNxIBbz009Io277hWQx6Yg58nqS24Qb64Bc2+qTbXAE5GgieBEcONQYe/
oV5Dd4VSdCnZ4cPLlRu+whJdy422LR07Snzj56VG+0SNzn01P16VWbCqwgke6aqXtkT3XZfi
Pr1rKkF9Jbu7bjvE+Z/tUbbfQ72B+H6UMfZF3hcQ/wAU/wB6FYrYeIJ0FsnkDH5AVlzN0w8h
nEbetfiWfEwfeKHX8dmzgQDqIDFtRI0J/KgWJ2JiFDMyqqjUsbiAAcyS2gqnYHVroQc2oIOm
U6gjnI+dY77m0uwXw1sHT61ijeD2F1gJWNPy5c6AYK7ypq2dafJKtB1jSZP5b6y1e50r7AHH
bOCyNKX8bag0e2hiZnhzpax+Ik0cedgXxuUHaWNet9AtoW1wVpWuIGBeVzAETcYiRzj8qR+h
2Ctu1w3EVzl0DCQNV1g+Zoftm29m+wsgqMoMKZ375HESDoaZYtoYf2iYQgrctFWTOSMsGGu6
MB/EY0qfoHgVRWxLkDMeptEwJGaGI8WfQeCUsYfbHWW3t3UE8LgADgmd07jurW1tttdtWbFp
erFjKVVGzSygBWzQJZd+7eTyrO4xKWnbuNO39r28Fefq8NbFx+0bzmSxedwHabUMIlRpypST
F3MdiVS5cgGT/KssQo3AwDHqTOpNvpN0kXE27avaAuqO0wYHUxOg3CQCBqeGmsrOHusjqyEh
9wI39oFdPGCRW1aBk9NL9S1tp7Av3BbzlAYGUrGgExqeM1lDbylWKlSCDBrKykDYXxbAOQNZ
JPvNFOj+E6y+o9he23kuoHqYpfud8/xN8zTj0I/138Nv5tWNDYy2Y44YcatNc+NVcP3R9cKk
ffXMFFpXOjDf9b6h2ntC1bUNccIG0Ezq3hAqN+76H/qFKfTE/cHzX5ius0aXxltEz9YMvP63
0JxPTGwhjNnPJNfjupJN5vsr9pvZ4nmaHbLUG7BEjLc0/ketW4MmPb9PbUaW29SI+dDsb08a
CLVvXmxhfcNT7xSUd9bFFQFljaW1Lt8/eOWHBdyA+W71OvjRLtJCMdVAA5ECACPCgZpl2frh
tdYXSdY31kuAoMu4BppqweIItkk6DX/FJGy9/p+tN+E/0R8qnlyNvYXsa8T4yd/Ol7Eb6N7R
73140BvfpTYGTY1dCmk3ddco08PoUF6WE/apmOyuvLVo/WiPRDvep/6GoZ0t/wDsf/mn50a5
FM6t2xdZQIzuQsz2TwB8PdU239kW1U5Lme7bUtdUcbYIExwyyPSfCl9O431xFNOxNTaJ1LZ5
PE6cedDVMNu0KFZJBkbwfjwra90elY35flTRJeuY3DMSXtNnPei42/jvNZRzD2lyJ2R3V4Dk
KylhWf/Z

--------------px0JXq3DNsdR43veRZqHptHO--
```


Las notas MIME (Multipurpose Internet Mail Extensions) permiten enviar correos electrónicos con contenido diverso, como texto, imágenes y archivos adjuntos.

Cuando un correo electrónico tiene el encabezado "Content-Type: multipart/mixed", significa que el mensaje consta de múltiples partes, algunas de las cuales pueden ser archivos adjuntos.

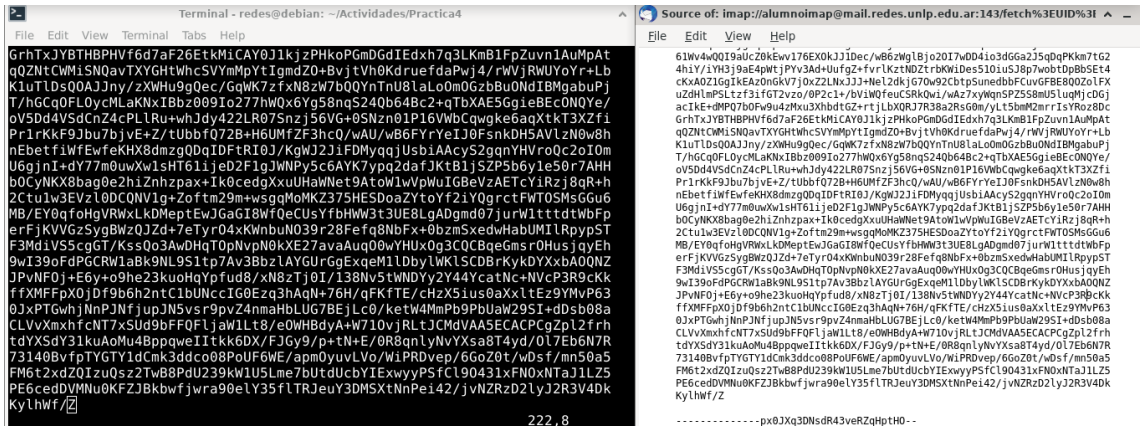
Para separar y marcar cada parte dentro de un mensaje MIME, se utiliza un identificador de límite llamado "boundary", que se establece en el encabezado "Content-Type".

Cada parte del mensaje se delimita con "--boundary", y el "boundary" actúa como un marcador para indicar dónde comienza y termina cada parte.

Debajo de cada divisor se encuentra de nuevo el encabezado Content-Type y otro llamado Content-Transfer-Encoding. Estos indican el tipo del contenido y el algoritmo usado para codificarlo y decodificarlo.

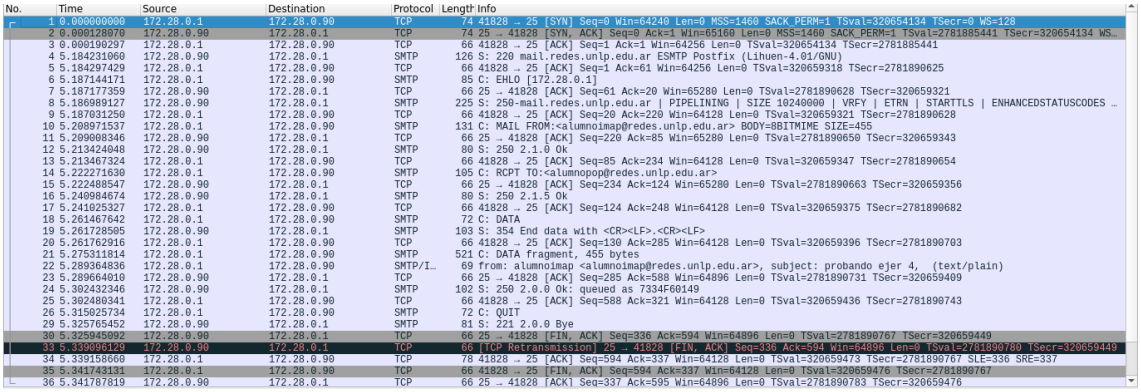
En este caso aparecen dos. El texto y la imagen.

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

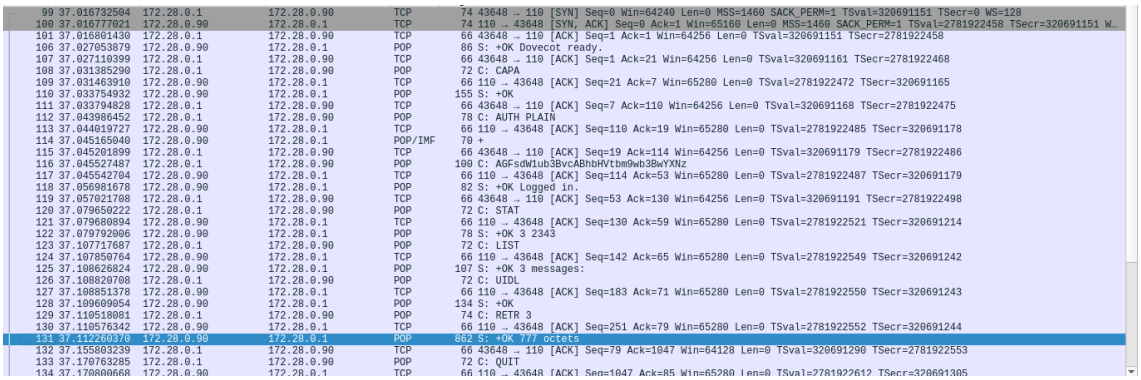


4. **Análisis del protocolo POP**
   a. **Utilizando Wireshark, capture el tráfico de red contra el servidor de correo mientras desde la cuenta alumnoimap@redes.unlp.edu.ar le envía una correo a alumnopop@redes.unlp.edu.ar y mientras alumnopop@redes.unlp.edu.ar recepciona dicho correo.**

Envio



Recepcion



```
 99 37.016732504  172.28.0.1      172.28.0.90     TCP       74 43648 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=320691151 TSecr=0 WS=128
100 37.016777021  172.28.0.90     172.28.0.1      TCP       74 110 → 43648 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=2781922450 TSecr=320691151 W…
101 37.016801430  172.28.0.1      172.28.0.90     TCP       66 43648 → 110 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=320691151 TSecr=2781922458
106 37.027053879  172.28.0.90     172.28.0.1      POP       86 S: +OK Dovecot ready.
107 37.027110399  172.28.0.1      172.28.0.90     TCP       66 43648 → 110 [ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=320691161 TSecr=2781922468
108 37.031385290  172.28.0.1      172.28.0.90     POP       72 C: CAPA
109 37.031463910  172.28.0.90     172.28.0.1      TCP       66 110 → 43648 [ACK] Seq=21 Ack=7 Win=65280 Len=0 TSval=2781922472 TSecr=320691165
110 37.033754932  172.28.0.90     172.28.0.1      POP      155 S: +OK
111 37.033794828  172.28.0.1      172.28.0.90     TCP       66 43648 → 110 [ACK] Seq=7 Ack=110 Win=64256 Len=0 TSval=320691168 TSecr=2781922475
112 37.043986452  172.28.0.1      172.28.0.90     POP       78 C: AUTH PLAIN
113 37.044019727  172.28.0.90     172.28.0.1      TCP       66 110 → 43648 [ACK] Seq=110 Ack=19 Win=65280 Len=0 TSval=2781922485 TSecr=320691178
114 37.045165040  172.28.0.90     172.28.0.1      POP/IMF   70 +
115 37.045201899  172.28.0.1      172.28.0.90     TCP       66 43648 → 110 [ACK] Seq=19 Ack=114 Win=64256 Len=0 TSval=320691179 TSecr=2781922486
116 37.045527487  172.28.0.1      172.28.0.90     POP      100 C: AGFsdW1ub3BvcABhbHVtbm9wb3BwYXNz
117 37.045542704  172.28.0.90     172.28.0.1      TCP       66 110 → 43648 [ACK] Seq=114 Ack=53 Win=65280 Len=0 TSval=2781922487 TSecr=320691179
118 37.056981678  172.28.0.90     172.28.0.1      POP       82 S: +OK Logged in.
119 37.057021708  172.28.0.1      172.28.0.90     TCP       66 43648 → 110 [ACK] Seq=53 Ack=130 Win=64256 Len=0 TSval=320691191 TSecr=2781922498
120 37.079650222  172.28.0.1      172.28.0.90     POP       72 C: STAT
121 37.079680894  172.28.0.90     172.28.0.1      TCP       66 110 → 43648 [ACK] Seq=130 Ack=59 Win=65280 Len=0 TSval=2781922521 TSecr=320691214
122 37.079792006  172.28.0.90     172.28.0.1      POP       78 S: +OK 3 2343
123 37.107717687  172.28.0.1      172.28.0.90     POP       72 C: LIST
124 37.107850764  172.28.0.90     172.28.0.1      TCP       66 110 → 43648 [ACK] Seq=142 Ack=65 Win=65280 Len=0 TSval=2781922549 TSecr=320691242
125 37.108626824  172.28.0.90     172.28.0.1      POP      107 S: +OK 3 messages:
126 37.108820708  172.28.0.1      172.28.0.90     POP       72 C: UIDL
127 37.108851378  172.28.0.90     172.28.0.1      TCP       66 110 → 43648 [ACK] Seq=183 Ack=71 Win=65280 Len=0 TSval=2781922550 TSecr=320691243
128 37.109609054  172.28.0.90     172.28.0.1      POP      134 S: +OK
129 37.110518081  172.28.0.1      172.28.0.90     POP       74 C: RETR 3
130 37.110576342  172.28.0.90     172.28.0.1      TCP       66 110 → 43648 [ACK] Seq=251 Ack=79 Win=65280 Len=0 TSval=2781922552 TSecr=320691244
131 37.112260370  172.28.0.90     172.28.0.1      POP      862 S: +OK 777 octets
132 37.155803239  172.28.0.1      172.28.0.90     TCP       66 43648 → 110 [ACK] Seq=79 Ack=1047 Win=64128 Len=0 TSval=320691290 TSecr=2781922553
133 37.170763285  172.28.0.1      172.28.0.90     POP       72 C: QUIT
134 37.170808668  172.28.0.90     172.28.0.1      TCP       66 110 → 43648 [ACK] Seq=1047 Ack=85 Win=65280 Len=0 TSval=2781922612 TSecr=320691305
```

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

```
+OK Dovecot ready.
CAPA
+OK
CAPA
TOP
UIDL
RESP-CODES
PIPELINING
AUTH-RESP-CODE
STLS
USER
SASL PLAIN
.
AUTH PLAIN
+
AGFsdW1ub3BvcABhbHVtbm9wb3BwYXNz
+OK Logged in.
STAT
+OK 3 2343
LIST
+OK 3 messages:
1 781
2 785
3 777
.
UIDL
+OK
1 0000000456eaa394
2 0000000556eaa394
3 0000000656eaa394
.
RETR 3
+OK 777 octets
Return-Path: <alumnoimap@redes.unlp.edu.ar>
X-Original-To: alumnopop@redes.unlp.edu.ar
Delivered-To: alumnopop@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 7334F60149
                    for <alumnopop@redes.unlp.edu.ar>; Tue, 12 Sep 2023 20:20:46 +0000 (UTC)
Message-ID: <1a58a149-391a-b218-7183-a1af6edac7b4@redes.unlp.edu.ar>
Date: Tue, 12 Sep 2023 17:20:41 -0300
MIME-Version: 1.0
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
 Thunderbird/91.12.0
Content-Language: en-US
To: alumnopop@redes.unlp.edu.ar
From: alumnoimap <alumnoimap@redes.unlp.edu.ar>
Subject: probando eier 4
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit

probando

.
QUIT
+OK Logging out.
```

Comandos:

- CAPA: El comando CAPA se utiliza para negociar una capa de seguridad (como SSL/TLS) entre el cliente POP3 y el servidor, lo que permite una conexión segura para el intercambio de correos electrónicos.

- AUTH PLAIN: AUTH PLAIN es un comando de autenticación que permite al cliente POP3 enviar su nombre de usuario y contraseña en un formato codificado en base64 para autenticarse en el servidor.

- STAT: El comando STAT se utiliza para obtener estadísticas sobre el buzón del usuario, incluyendo el número total de mensajes en el buzón y el tamaño total en octetos.

- LIST: El comando LIST se utiliza para obtener una lista de los mensajes en el buzón junto con sus tamaños. También se puede usar para obtener información sobre un mensaje específico proporcionando su número.
-
  UIDL: El comando UIDL se utiliza para obtener una lista de los identificadores únicos de los mensajes en el buzón. Estos identificadores son útiles para realizar un seguimiento de mensajes específicos.

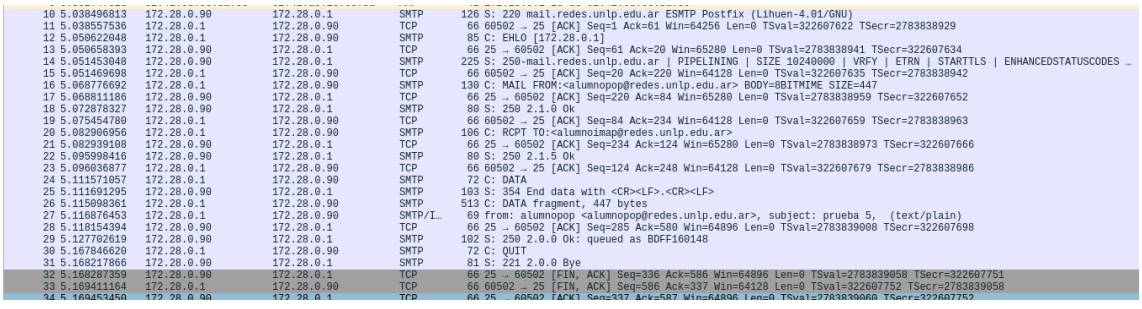
- RETR: El comando RETR se utiliza para recuperar un mensaje específico del buzón por su número. Permite al cliente obtener el contenido completo de un mensaje para su lectura.

- QUIT: El comando QUIT se utiliza para finalizar una sesión POP3 de manera ordenada. Una vez enviado, el servidor cierra la conexión y el cliente se desconecta.

5. Análisis del protocolo IMAP

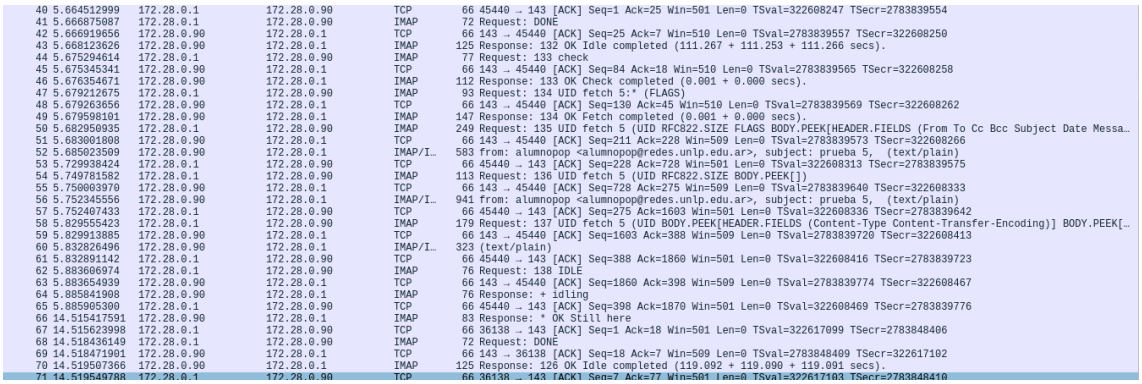
a. Utilizando Wireshark, capture el tráfico de red contra el servidor de correo mientras desde la cuenta alumnopop@redes.unlp.edu.ar le envía una correo a alumnoimap@redes.unlp.edu.ar y mientras alumnoimap@redes.unlp.edu.ar recepciona dicho correo.}

Envio



10	5.038496813	172.28.0.90	172.28.0.1	SMTP	126 S: 220 mail.redes.unlp.edu.ar ESMTP Postfix (Lihuen-4.01/GNU)
11	5.038557536	172.28.0.1	172.28.0.90	TCP	66 60502 → 25 [ACK] Seq=1 Ack=61 Win=64256 Len=0 TSval=322607622 TSecr=2783838929
12	5.050622048	172.28.0.1	172.28.0.90	SMTP	85 C: EHLO [172.28.0.1]
13	5.050658393	172.28.0.90	172.28.0.1	TCP	66 25 → 60502 [ACK] Seq=61 Ack=20 Win=65280 Len=0 TSval=2783838941 TSecr=322607634
14	5.051453048	172.28.0.90	172.28.0.1	SMTP	225 S: 250-mail.redes.unlp.edu.ar | PIPELINING | SIZE 10240000 | VRFY | ETRN | STARTTLS | ENHANCEDSTATUSCODES …
15	5.051469698	172.28.0.1	172.28.0.90	TCP	66 60502 → 25 [ACK] Seq=20 Ack=220 Win=64128 Len=0 TSval=322607635 TSecr=2783838942
16	5.068776692	172.28.0.1	172.28.0.90	SMTP	130 C: MAIL FROM:<alumnopop@redes.unlp.edu.ar> BODY=8BITMIME SIZE=447
17	5.068811186	172.28.0.90	172.28.0.1	TCP	66 25 → 60502 [ACK] Seq=220 Ack=84 Win=65280 Len=0 TSval=2783838959 TSecr=322607652
18	5.072878327	172.28.0.90	172.28.0.1	SMTP	80 S: 250 2.1.0 Ok
19	5.075454780	172.28.0.1	172.28.0.90	TCP	66 60502 → 25 [ACK] Seq=84 Ack=234 Win=64128 Len=0 TSval=322607659 TSecr=2783838963
20	5.082906956	172.28.0.1	172.28.0.90	SMTP	106 C: RCPT TO:<alumnoimap@redes.unlp.edu.ar>
21	5.082939108	172.28.0.90	172.28.0.1	TCP	66 25 → 60502 [ACK] Seq=234 Ack=124 Win=65280 Len=0 TSval=2783838973 TSecr=322607666
22	5.095998416	172.28.0.90	172.28.0.1	SMTP	80 S: 250 2.1.5 Ok
23	5.096036877	172.28.0.1	172.28.0.90	TCP	66 60502 → 25 [ACK] Seq=124 Ack=248 Win=64128 Len=0 TSval=322607679 TSecr=2783838986
24	5.111571057	172.28.0.1	172.28.0.90	SMTP	72 C: DATA
25	5.111691295	172.28.0.90	172.28.0.1	SMTP	103 S: 354 End data with <CR><LF>.<CR><LF>
26	5.115098361	172.28.0.1	172.28.0.90	SMTP	513 C: DATA fragment, 447 bytes
27	5.116876453	172.28.0.1	172.28.0.90	SMTP/I…	69 from: alumnopop <alumnopop@redes.unlp.edu.ar>, subject: prueba 5, (text/plain)
28	5.118154394	172.28.0.90	172.28.0.1	TCP	66 25 → 60502 [ACK] Seq=285 Ack=580 Win=64896 Len=0 TSval=2783839008 TSecr=322607698
29	5.127702619	172.28.0.90	172.28.0.1	SMTP	102 S: 250 2.0.0 Ok: queued as BDFF160148
30	5.167846620	172.28.0.1	172.28.0.90	SMTP	72 C: QUIT
31	5.168217866	172.28.0.90	172.28.0.1	SMTP	81 S: 221 2.0.0 Bye
32	5.168287359	172.28.0.90	172.28.0.1	TCP	66 25 → 60502 [FIN, ACK] Seq=336 Ack=586 Win=64896 Len=0 TSval=2783839058 TSecr=322607751
33	5.169411164	172.28.0.1	172.28.0.90	TCP	66 60502 → 25 [FIN, ACK] Seq=586 Ack=337 Win=64128 Len=0 TSval=322607752 TSecr=2783839058
34	5.169453450	172.28.0.90	172.28.0.1	TCP	66 25 → 60502 [ACK] Seq=337 Ack=587 Win=64896 Len=0 TSval=2783839060 TSecr=322607752

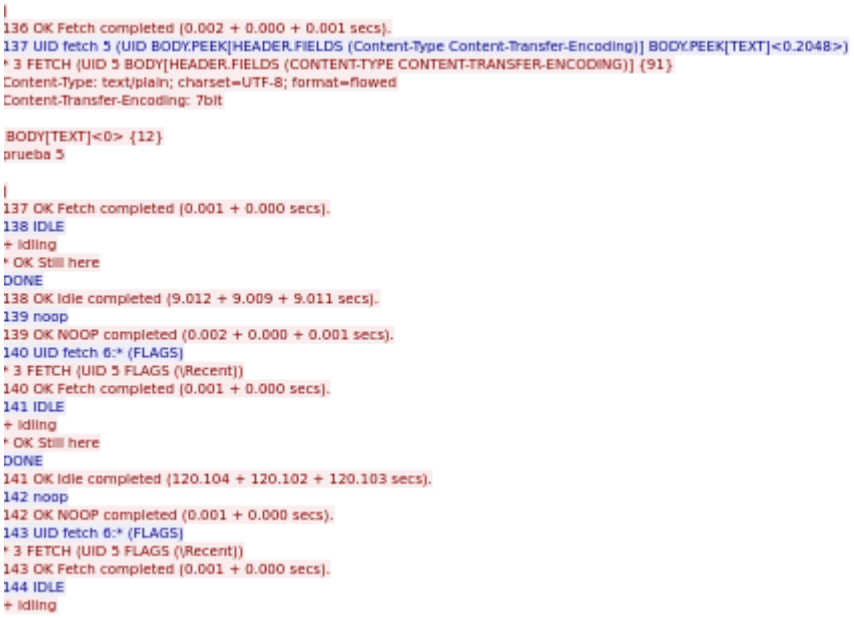
Recepcion



```
    40 5.664512999   172.28.0.1      172.28.0.90     TCP       66 45440 → 143 [ACK] Seq=1 Ack=25 Win=501 Len=0 TSval=322608247 TSecr=2783839554
    41 5.666875087   172.28.0.1      172.28.0.90     IMAP      72 Request: DONE
    42 5.666919656   172.28.0.90     172.28.0.1      TCP       66 143 → 45440 [ACK] Seq=25 Ack=7 Win=510 Len=0 TSval=2783839557 TSecr=322608250
    43 5.668123626   172.28.0.90     172.28.0.1      IMAP     125 Response: 132 OK Idle completed (111.267 + 111.253 + 111.266 secs).
    44 5.675294614   172.28.0.1      172.28.0.90     IMAP      77 Request: 133 check
    45 5.675345341   172.28.0.90     172.28.0.1      TCP       66 143 → 45440 [ACK] Seq=84 Ack=18 Win=510 Len=0 TSval=2783839565 TSecr=322608258
    46 5.676354671   172.28.0.90     172.28.0.1      IMAP     112 Response: 133 OK Check completed (0.001 + 0.000 secs).
    47 5.679212675   172.28.0.1      172.28.0.90     IMAP      93 Request: 134 UID fetch 5:* (FLAGS)
    48 5.679263656   172.28.0.90     172.28.0.1      TCP       66 143 → 45440 [ACK] Seq=130 Ack=45 Win=510 Len=0 TSval=2783839569 TSecr=322608262
    49 5.679598101   172.28.0.90     172.28.0.1      IMAP     147 Response: 134 OK Fetch completed (0.001 + 0.000 secs).
    50 5.682950935   172.28.0.1      172.28.0.90     IMAP     249 Request: 135 UID fetch 5 (UID RFC822.SIZE FLAGS BODY.PEEK[HEADER.FIELDS (From To Cc Bcc Subject Date Messa…
    51 5.683001808   172.28.0.90     172.28.0.1      TCP       66 143 → 45440 [ACK] Seq=211 Ack=228 Win=509 Len=0 TSval=2783839573 TSecr=322608266
    52 5.685023509   172.28.0.90     172.28.0.1      IMAP/I…  583 from: alumnopop <alumnopop@redes.unlp.edu.ar>, subject: prueba 5,  (text/plain)
    53 5.729938424   172.28.0.1      172.28.0.90     TCP       66 45440 → 143 [ACK] Seq=228 Ack=728 Win=501 Len=0 TSval=322608313 TSecr=2783839575
    54 5.749781582   172.28.0.1      172.28.0.90     IMAP     113 Request: 136 UID fetch 5 (UID RFC822.SIZE BODY.PEEK[])
    55 5.750003970   172.28.0.90     172.28.0.1      TCP       66 143 → 45440 [ACK] Seq=728 Ack=275 Win=509 Len=0 TSval=2783839640 TSecr=322608333
    56 5.752345556   172.28.0.90     172.28.0.1      IMAP/I…  941 from: alumnopop <alumnopop@redes.unlp.edu.ar>, subject: prueba 5,  (text/plain)
    57 5.752407433   172.28.0.1      172.28.0.90     TCP       66 45440 → 143 [ACK] Seq=275 Ack=1603 Win=501 Len=0 TSval=322608336 TSecr=2783839642
    58 5.829555423   172.28.0.1      172.28.0.90     IMAP     179 Request: 137 UID fetch 5 (UID BODY.PEEK[HEADER.FIELDS (Content-Type Content-Transfer-Encoding)] BODY.PEEK[…
    59 5.829913885   172.28.0.90     172.28.0.1      TCP       66 143 → 45440 [ACK] Seq=1603 Ack=388 Win=509 Len=0 TSval=2783839720 TSecr=322608413
    60 5.832826496   172.28.0.90     172.28.0.1      IMAP/I…  323 (text/plain)
    61 5.832891142   172.28.0.1      172.28.0.90     TCP       66 45440 → 143 [ACK] Seq=388 Ack=1860 Win=501 Len=0 TSval=322608416 TSecr=2783839723
    62 5.883606974   172.28.0.1      172.28.0.90     IMAP      76 Request: 138 IDLE
    63 5.883654939   172.28.0.90     172.28.0.1      TCP       66 143 → 45440 [ACK] Seq=1860 Ack=398 Win=509 Len=0 TSval=2783839774 TSecr=322608467
    64 5.885841908   172.28.0.90     172.28.0.1      IMAP      76 Response: + idling
    65 5.885905300   172.28.0.1      172.28.0.90     TCP       66 45440 → 143 [ACK] Seq=398 Ack=1870 Win=501 Len=0 TSval=322608469 TSecr=2783839776
    66 14.515417591  172.28.0.90     172.28.0.1      IMAP      83 Response: * OK Still here
    67 14.515623998  172.28.0.1      172.28.0.90     TCP       66 36138 → 143 [ACK] Seq=1 Ack=18 Win=501 Len=0 TSval=322617099 TSecr=2783848406
    68 14.518436149  172.28.0.1      172.28.0.90     IMAP      72 Request: DONE
    69 14.518471901  172.28.0.90     172.28.0.1      TCP       66 143 → 36138 [ACK] Seq=18 Ack=7 Win=509 Len=0 TSval=2783848409 TSecr=322617102
    70 14.519507366  172.28.0.90     172.28.0.1      IMAP     125 Response: 126 OK Idle completed (119.092 + 119.090 + 119.091 secs).
    71 14.519549788  172.28.0.1      172.28.0.90     TCP       66 36138 → 143 [ACK] Seq=7 Ack=77 Win=501 Len=0 TSval=322617103 TSecr=2783848410
```

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.

```
* 3 EXISTS
* 1 RECENT
DONE
132 OK Idle completed (111.267 + 111.253 + 111.266 secs).
133 check
133 OK Check completed (0.001 + 0.000 secs).
134 UID fetch 5:* (FLAGS)
* 3 FETCH (UID 5 FLAGS (\Recent))
134 OK Fetch completed (0.001 + 0.000 secs).
135 UID fetch 5 (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)])
* 3 FETCH (UID 5 RFC822.SIZE 771 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)] {267}
Message-ID: <d5c7f272-efad-03ca-508d-b6ffa7d78cdb@redes.unlp.edu.ar>
Date: Tue, 12 Sep 2023 17:53:09 -0300
To: alumnoimap@redes.unlp.edu.ar
From: alumnopop <alumnopop@redes.unlp.edu.ar>
Subject: prueba 5
Content-Type: text/plain; charset=UTF-8; format=flowed

)
135 OK Fetch completed (0.002 + 0.000 + 0.001 secs).
136 UID fetch 5 (UID RFC822.SIZE BODY.PEEK[])
* 3 FETCH (UID 5 RFC822.SIZE 771 BODY[] {771}
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 BDFF160148
                for <alumnoimap@redes.unlp.edu.ar>; Tue, 12 Sep 2023 20:53:14 +0000 (UTC)
Message-ID: <d5c7f272-efad-03ca-508d-b6ffa7d78cdb@redes.unlp.edu.ar>
Date: Tue, 12 Sep 2023 17:53:09 -0300
MIME-Version: 1.0
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
 Thunderbird/91.12.0
Content-Language: en-US
To: alumnoimap@redes.unlp.edu.ar
From: alumnopop <alumnopop@redes.unlp.edu.ar>
Subject: prueba 5
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit

prueba 5

)
136 OK Fetch completed (0.002 + 0.000 + 0.001 secs).
137 UID fetch 5 (UID BODY.PEEK[HEADER.FIELDS (Content-Type Content-Transfer-Encoding)] BODY.PEEK[TEXT]<0.2048>)
* 3 FETCH (UID 5 BODY[HEADER.FIELDS (CONTENT-TYPE CONTENT-TRANSFER-ENCODING)] {91}
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit

 BODY[TEXT]<0> {12}
prueba 5

)
```



Comandos:

- DONE: El comando DONE se utiliza para indicar que se ha completado una transacción abierta en el servidor IMAP. Puede usarse para confirmar la finalización de una secuencia de comandos o transacción previamente iniciada.

- CHECK: El comando CHECK se utiliza para verificar la integridad de una carpeta IMAP y asegurarse de que todos los cambios pendientes se han aplicado correctamente. Es útil para garantizar la coherencia de la información en el servidor IMAP.

- UID CHECK: Similar a CHECK, pero se aplica a mensajes específicos identificados por sus identificadores únicos (UID). Permite verificar y sincronizar mensajes específicos en lugar de toda la carpeta.

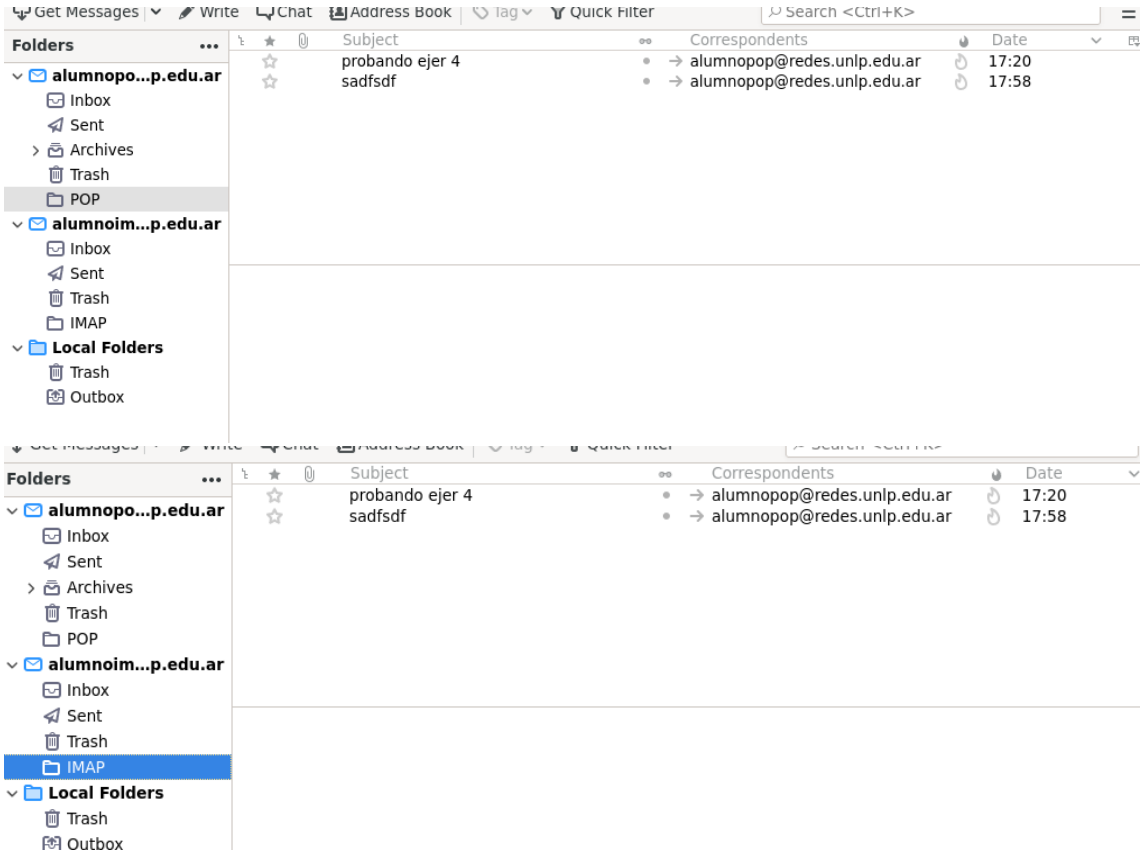
- UID FETCH: El comando UID FETCH se utiliza para recuperar información específica de un mensaje de correo electrónico en una carpeta IMAP, identificándolo mediante su identificador único (UID). Esto permite un acceso preciso a mensajes individuales.

    - UID FETCH 5:: El cliente solicita al servidor que recupere información sobre los mensajes con identificadores únicos (UID) desde el mensaje 5 en adelante.
    - UID FETCH 5 (UID RFC822.SIZE FLAGS BODY.PEEK[HEADER.FIELDS...): El cliente solicita información detallada sobre el mensaje con UID 5, incluyendo su tamaño, banderas y encabezado.
    - UID FETCH 5 (UID RFC822.SIZE BODY.PEEK[]): El cliente solicita el cuerpo completo del mensaje con UID 5.
    - UID FETCH 5 (UID BODY.PEEK[HEADER.FIELDS...): El cliente solicita información específica del encabezado del mensaje con UID 5.

- IDLE: El comando IDLE permite al cliente IMAP mantener una conexión abierta con el servidor mientras espera notificaciones de nuevos mensajes. Cuando se usa IDLE, el servidor informa inmediatamente al cliente cuando llega un nuevo correo, lo que facilita notificaciones en tiempo real.

- NOOP: El comando NOOP (No Operation) es una solicitud simple al servidor IMAP que no realiza ninguna acción significativa. Se utiliza principalmente para mantener una conexión activa sin realizar cambios en el estado de la carpeta o los mensajes. Puede ser útil para mantener la sesión IMAP abierta.

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 el caso de alumnopop veo los recibidos (no los enviados) y están marcados como no leídos.

   En el caso de alumnoimap veo los recibidos y los enviados (marcados como leídos).

   Con respecto a porque no están marcados como leidos en POP3 los correos electrónicos se descargan del servidor al cliente y se marcan como no leídos en el cliente, mientras que en el protocolo IMAP, los correos se almacenan en el servidor y se reflejan en el cliente. Los correos enviados se consideran leídos porque ya se enviaron desde el cliente. IMAP sincroniza el estado de los correos electrónicos entre el cliente y el servidor.

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

   La de POP no esta pero la de IMAP si. Esto se debe a que POP3 no admite la sincronización de carpetas en el servidor (están localmente), mientras que IMAP permite acceder y sincronizar todas las carpetas en el servidor.

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?**

   Considero que es mejor IMAP ya que es más completo y adecuado si se quiere una experiencia de correo electrónico más sincronizada entre múltiples dispositivos (lo que la mayoría desea) y se necesita acceder a carpetas en el servidor. Permite trabajar desde varios dispositivos y mantener una estructura de carpetas consistente.
   En cuanto a los recursos del servidor, IMAP generalmente requiere más recursos debido a su capacidad de mantener el estado de los correos electrónicos y la estructura de carpetas en el servidor. Sin embargo, la mayoría de los servidores de correo modernos están diseñados para gestionar eficientemente esta carga de trabajo adicional.

7. **¿En algún caso es posible enviar más de un correo durante una misma conexión tcp?**
   Considere:
   Destinatarios múltiples del mismo dominio entre MUA-MSA y entre MTA-MTA

Destinatarios múltiples de diferentes dominios entre MUA-MSA y entre MTA MTA

Destinatarios múltiples del mismo dominio entre MUA-MSA: En una misma conexión TCP, un MUA (Agente de Usuario de Correo) puede enviar varios correos electrónicos a destinatarios que pertenecen al mismo dominio y que son manejados por el mismo servidor MSA (Agente de Transferencia de Correo de Salida). Esto se debe a que el MSA puede aceptar varios correos en una sola conexión TCP antes de cerrarla, lo que ahorra recursos y reduce la sobrecarga de establecer múltiples conexiones TCP.

Destinatarios múltiples de diferentes dominios entre MUA-MSA y entre MTA-MTA: En el caso de enviar correos a destinatarios en diferentes dominios, es posible que se utilicen múltiples conexiones TCP durante el proceso de envío de correos. Cada conexión TCP puede estar asociada con un MSA o un MTA (Agente de Transferencia de Correo de Salida o Agente de Transferencia de Correo de Relevo) diferente, dependiendo de cómo se enrutó el correo hacia su destino final. Por lo tanto, para enviar correos a destinatarios en diferentes dominios, es probable que se establezcan múltiples conexiones TCP a diferentes servidores MSA o MTA, una para cada dominio de destino.

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

   Sí, un MSA (Agente de Transferencia de Correo de Salida) puede escuchar en un puerto TCP diferente a los convencionales. Esto puede proporcionar seguridad adicional al evitar ataques dirigidos a los puertos estándar, prevenir conflictos de puertos con otros servicios y permitir una personalización más granular de la configuración del servidor de correo. Sin embargo, se deben considerar las implicancias, como la necesidad de configurar los clientes para utilizar el puerto personalizado, posibles problemas de interoperabilidad y posibles bloqueos por parte de firewalls y filtros de correo electrónico.

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

   Sí, es posible configurar un MTA (Agente de Transferencia de Correo de Relevo) para que escuche en un puerto TCP diferente al convencional (por ejemplo, el puerto 25). Esto puede proporcionar seguridad adicional al ocultar el MTA de escaneos y ataques automatizados dirigidos al puerto estándar. Sin embargo, implica que los clientes y otros servidores de correo deben configurarse para utilizar el puerto específico y puede requerir ajustes en firewalls y enrutadores para permitir el tráfico en ese puerto.

   (Preguntar diferencias entre MSA Y MTA)

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 envíar 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?

Debería informarle al servidor autoritativo de .com.ar:

- El *NS* de los servidores autoritativos del dominio redes2022.com.ar (ns1 y ns2)
- El *A* de ambos servidores autoritativos.

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.

Seria necesario configurar en el NS los siguientes registros:

- redes2022.com.ar 86400 IN NS ns1.redes2022.com.ar
- redes2022.com.ar 86400 IN NS ns2.redes2022.com.ar

- redes2022.com.ar 86400 IN MX 5 mail.redes2022.com.ar

- ns1.redes2022.com.ar 86400 IN A 203.0.113.65
- ns2.redes2022.com.ar 86400 IN A 203.0.113.66
- mail.redes2022.com.ar 86400 IN A 203.0.113.111
- www.webmail.redes2022.com.ar 86400 IN A 203.0.113.8

- redes2022.com.ar 86400 IN SOA ns1.redes2022.com.ar root.redes2022.com.ar 2023091300 604800 86400 2419200 86400

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

No, no es necesario, puede aceptar una consulta iterativa o recursiva, pero de igual manera responderá recursivamente ya que al ser el servidor autoritativo es el dueño de los dominios por los que se esta consultando por lo que respondería de forma recursiva.

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

En los servidores DNS cconfiguraria el protocolo DNS, en el servidor de correo configuraría el SMTP e IMAP y en el servidor web el HTTPS.

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.

ns1/ns2 – UDP o TCP (en caso de que la respuesta exceda 512 bytes) – 53
correo – TCP – 80 (http) o 443 (https)
mail – TCP – 25 (SMTP), 110 (POP3) y 143 (IMAP).

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

El webmail actuaria como MUA y se conectaría con el servidor de correo local usando el protocolo SMTP para enviar el mail y este (con el mismo protocolo) se lo enviaría al servidor de mail remoto.
Para recibir correos, el webmail utilizaría los protocolos IMAP o POP3 para recuperar los mensajes del servidor de correo, para eso necesitar autenticación.
El cliente (las personas) se conectaría al webmail haciendo uso del protocolo HTTP (o HTTPS)

g) ¿Cómo se podría hacer para que cualquier MTA reconozca como válidos los mails provienentes 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.

Se debería configurar en el registro SPF del servidor DNS primario con el dominio redes2022.com.ar y la dirección 203.0.113.111. Si, afectaría esto a los mails enviados desde la webmail, ya que esta estaría enviando los mails al servidor de mail local y este servidor de mail local se lo enviara al servidor de correo remoto. Como la ip del servidor de mail local no se encuentra en el SPF, el servidor remoto no lo aceptara.

(consultar)

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)?

Fueron diseñados originalmente para el envío de texto plano y caracteres ASCII.

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**

Si, se podría cambiando el encabezado “From”, ya que los protocolos de correo electrónico, como SMTP, no tienen un mecanismo integrado para verificar si la dirección del remitente es realmente quien dice ser.
En la actualidad existen certificados digitales que ayudan a mitigar la suplantación de identidad en el correo electrónico y en otras comunicaciones en línea

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**

No es posible enviar un correo electrónico de modo que el receptor vea que el destinatario es un usuario distinto. En los protocolos de correo electrónico como SMTP el encabezado "To" para indicar quién es el destinatario real del mensaje, y esta información no puede ser falsificada en el nivel del remitente de manera que el receptor vea otro destinatario.

Si no le llegaría al destinario que el receptor ve, esto podría ser un problema técnico, no una indicación de una estafa (ya que el encabezado “To” no se puede modificar).

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?**

Usara el protocolo SMTP. Se conectará con el servidor de correo local y este se conectará con el servidor de correo remoto del dominio info.unlp.edu.ar. Para ello el servidor de correo local deberá consultar por el registro MX al servidor autoritativo de info.unlp.edu.ar, conseguir la ip del IP y enviar el correo por prioridad al MTA correspondiente.

l) **Dado que solo disponemos de un servidor de correo, ¿qué sucederá con los mails que intenten ingresar durante un reinicio del servidor?**

El servidor de correo local los encolara hasta que puedan ser enviados.

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?**

      Debería agregar otro registro MX y A de tal manera que quede:

      redes2022.com.ar 86400 IN MX 10 nube.redes2022.com.ar
      nube.redes2022.com.ar 86400 IN A IP

Si se cae el servidor de correo con mayor prioridad (5) se enviarán a este servidor en la nube.

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 los fuentes del mensaje recibido para responder las siguientes preguntas:**

```
redes@debian:~$ swaks --to "alumnoimap@redes.unlp.edu.ar" --from "redesycomunicaciones@redes.unlp.edu.ar"
--h-Subject="SMTP-Practica4" --body="Esto es una prueba del protocolo SMTP" --server="mail.redes.unlp.edu.
ar" --attach /home/redes/Downloads/p04.pdf
```

    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.**

```
220 mail.redes.unlp.edu.ar ESMTP Postfix (Lihuen-4.01/GNU)
EHLO debian
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:<redesycomunicaciones@redes.unlp.edu.ar>
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>
Date: Wed, 13 Sep 2023 12:58:47 -0300
To: alumnoimap@redes.unlp.edu.ar
From: redesycomunicaciones@redes.unlp.edu.ar
Subject: SMTP-Practica4
Message-Id: <20230913125847.005385@debian>
X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----=_MIME_BOUNDARY_000_5385"

------=_MIME_BOUNDARY_000_5385
Content-Type: text/plain

Esto es una prueba del protocolo SMTP
------=_MIME_BOUNDARY_000_5385
Content-Type: application/octet-stream; name="p04.pdf"
```

La información enviada por el servidor destino como respuesta al comando EHLO corresponde a las capacidades y extensiones soportadas por el servidor de correo.

STARTTLS: Esta extensión indica que el servidor de correo es compatible con la encriptación TLS

CHUNKING: Esta extensión indica que el servidor de correo permite la transmisión eficiente y segura de correos electrónicos en fragmentos más pequeños

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

Date: Wed, 13 Sep 2023 12:58:47 -0300
To: alumnoimap@redes.unlp.edu.ar
From: redesycomunicaciones@redes.unlp.edu.ar
Subject: SMTP-Practica4
Message-Id: <20230913125847.005385@debian>
X-Mailer: swaks v20201014.0
jetmore.org/john/code/swaks/
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----=_MIME_BOUNDARY_000_5385"

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

Es 20230913125847.005385@debian, lo asigna el MUA

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

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

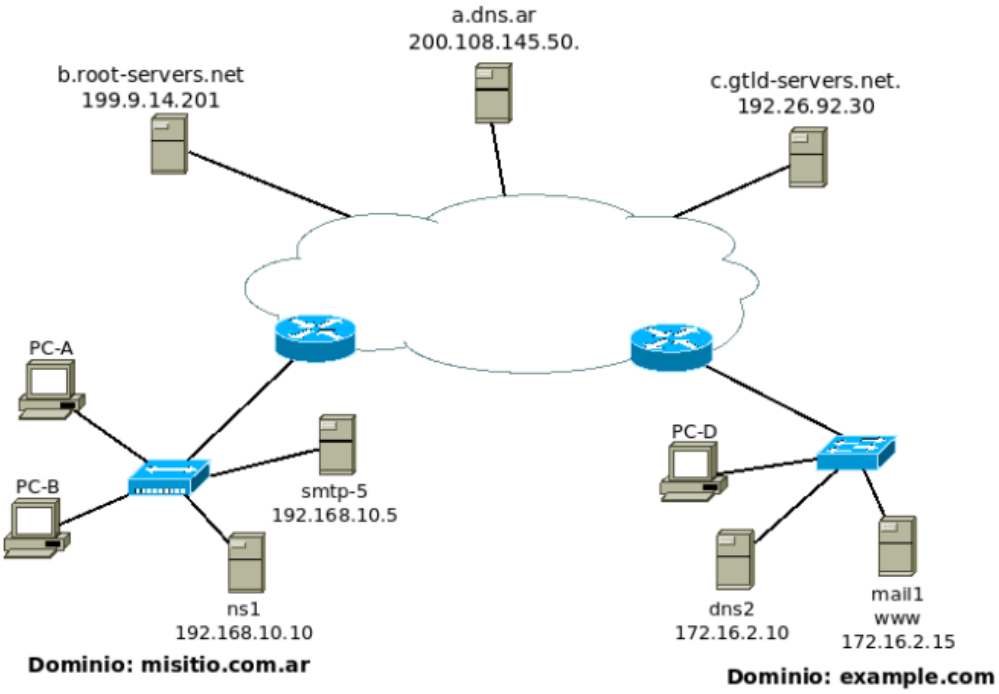
Es Postfix

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

```
Return-Path: <redesycomunicaciones@redes.unlp.edu.ar>
X-Original-To: alumnoimap@redes.unlp.edu.ar
Delivered-To: alumnoimap@redes.unlp.edu.ar
Received: from debian (unknown [172.28.0.1])
    by mail.redes.unlp.edu.ar (Postfix) with ESMTP id CA6E860169
    for <alumnoimap@redes.unlp.edu.ar>; Wed, 13 Sep 2023 15:58:52 +0000 (UTC)
Date: Wed, 13 Sep 2023 12:58:47 -0300
To: alumnoimap@redes.unlp.edu.ar
From: redesycomunicaciones@redes.unlp.edu.ar
Subject: SMTP-Practica4
Message-Id: <20230913125847.005385@debian>
X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----=_MIME_BOUNDARY_000_5385"

------=_MIME_BOUNDARY_000_5385
Content-Type: text/plain

Esto es una prueba del protocolo SMTP
------=_MIME_BOUNDARY_000_5385
Content-Type: application/octet-stream; name="p04.pdf"
Content-Description: p04.pdf
Content-Disposition: attachment; filename="p04.pdf"
Content-Transfer-Encoding: BASE64

JVBERi0xLjUKJdDUxdgKNiAwIG9iago8PC9MZW5ndGggMTYwMCAgICAgIC9GaWx0ZXIvRmxhdGVE
ZWNvZGU+PgpzdHJlYW0KeNqtWNtu20YQfddX8EJ6WkuX1E2TokGd0rVToIjzQJ0SoAiFV6c
uF/f2ZtESrIkI4IB7212dubsnNmhcLSIcPTb7Jeb2ct3jEUJ0lKyJLq5jwgsYPivMEqkjJTQKGE6
ullGn+M36Sqdv6AqifPCtRergszSrLxlktVmSsUv3Mqbpm2LxvWLqsj6lsqUGcwRKZiM/yryonMC
```

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?**
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?**
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"**

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



- **El usuario juan@misitio.com.ar en PC-A desea enviar un mail al usuario alicia@example.com**

- **Cada organización tiene su propios servidores de DNS y Mail**
-
- **El servidor ns1 no tiene la recursión habilitada para consultas realizadas desde fuera del dominio misitio.com.ar**

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?**

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

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

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?**

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

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**

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

- **Cada protocolo de la capa de aplicación agregará una cabecera con información propia de ese protocolo**
- **Como son todos protocolos de la capa de aplicación, las cabeceras agregadas por el protocolo de DNS puede ser analizadas y comprendidas por el protocolo SMTP o HTTP**

- **Para que los cliente en misitio.com.ar puedan acceder el servidor HTTP www.example.com y mostrar correctamente su contenido deben tener el mismo sistema operativo.**

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

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

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