

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 el envío 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

Datos para POP

- Cuenta de correo: **alumnopop@redes.unlp.edu.ar**
- Nombre de usuario: **alumnopop**
- Contraseña: **alumnopoppass**
- Puerto: **110**

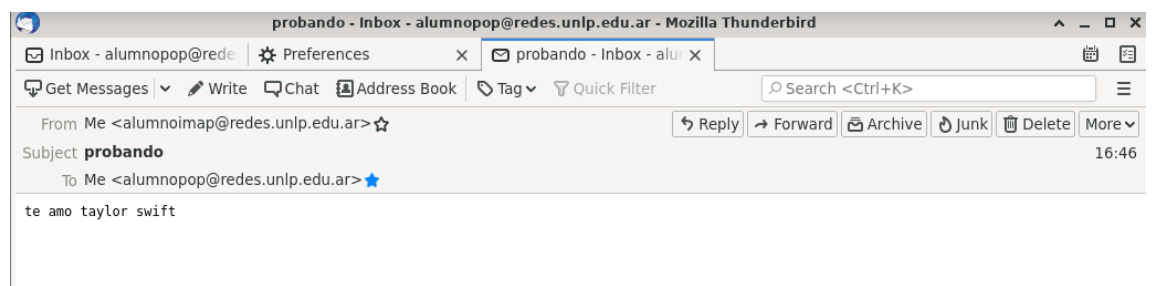
Datos para IMAP

- 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**
 - 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. . .

No.	Time	Source	Destination	Protocol	Length	Info
102	44.335460795	172.28.0.90	172.28.0.1	SMTP	126	S: 220 mail.redes.unlp.edu.ar ESMTP Postfix (Lihuen-4.01/GNU)
104	44.397253940	172.28.0.1	172.28.0.90	SMTP	85	C: EHLO [172.28.0.1]
106	44.387433793	172.28.0.90	172.28.0.1	SMTP	225	S: 250-mail.redes.unlp.edu.ar PIPELINING SIZE 10240000 VRFY ETRN STARTTLS ENHANCEDSTATUSCODES ...
108	44.397122757	172.28.0.1	172.28.0.90	SMTP	130	C: MAIL FROM:<alumnopop@redes.unlp.edu.ar> BODY=8BITMIME SIZE=467
110	44.402087749	172.28.0.90	172.28.0.1	SMTP	80	S: 250 2.1.0 Ok
112	44.422514182	172.28.0.1	172.28.0.90	SMTP	106	C: RCPT TO:<alumnoimap@redes.unlp.edu.ar>
114	44.430445785	172.28.0.90	172.28.0.1	SMTP	88	S: 250 2.1.5 Ok
116	44.437447188	172.28.0.1	172.28.0.90	SMTP	72	C: DATA
117	44.437911068	172.28.0.90	172.28.0.1	SMTP	103	S: 354 End data with <CR><LF>.<CR><LF>
119	44.440538198	172.28.0.1	172.28.0.90	SMTP	533	C: DATA fragment, 467 bytes
120	44.450837518	172.28.0.1	172.28.0.90	SMTP/I...	69	from: alumnopop <alumnopop@redes.unlp.edu.ar>, subject: estoy probando, (text/plain)
122	44.465270922	172.28.0.90	172.28.0.1	SMTP	102	S: 250 2.0.0 Ok: queued as 42E8C6010E
124	44.493565528	172.28.0.1	172.28.0.90	SMTP	72	C: QUIT
125	44.498399771	172.28.0.90	172.28.0.1	SMTP	81	S: 221 2.0.0 Bye

```
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.

/9j/4AAQSkZJRgABAQAAAQABAAD/2wCEAAoHCBUVFBcUFRUYGBcZGxocGhoaGRwgGhsZGh0a
GhkchSEiICwkHBwoIBkZJDUKKC0vMjIyGiI4PTgxPCwxMi8BCwsLDw4PHRERHTeOiygxMTEx
MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMf/AABEIARoA
swMBIGACEQEDEQH/xAAcAAACAgMBAQAAAAAAAAAAAAAFBgMEAACEBwj/xABFEAACQIDBAcf
BQCACgMBAABAHAAWQSIIQuXQVEGEyIyYXGBQPghsfAU1ILB0QdicoKS4fEzQ1Nzk6Kys8LS
JDSDFf/EABkBAAMBAQEAAAAAAAAAAAAAIDBAEABf/EADARAICAQMDAwIFAwUAAAAAAAAAB
AhEDEiExBEFRE2FxIQEUgZGx8DLR4RUzQLLB/9oADAMBAAIRAxEAPwBg6/IAZAMDix9+6sTF
XN+aV/EoUx6mY9aDLTG0ey7FD0X7zsgndpnAnwg6lbcG2cluyI1AMA+R/PhTVT4JHa5Ke3bn
xbixbdwy4vMrGEyiWTMBu9tc3MpvgLXdnpbuJmEvCMysYKN+Fq0InxB3qOkAvr20L2Nvc3Yf

61Wv4wQQ19aUcZ0kEwv1/6EX0KJJ1Dec/wB6ZwgLBjo201/wDD41o3dGGA2J5QDqPKkm/tG2
4hiY/iYH3j9aE4pWtjPYv3Ad+UufgZ+fvrLKztNDZtrbKWides510iuSj8p7wobtdpBbSEt4
cKxA0Z1GgIkEAzOnGkV7j0xZ2LNxJJJ+Ne12dkjG70w92CbtP5unedbbFCuvGFBE8Q0ZolFX
uZdHlmpSLtZf3ifGT2vzo/0P2c1+/bViWQfeuCSRkQwi/wAz7xyWqnSPZ5S8mU5luqMjcdGj
acIkE+dMPQ7b0Fw9u4zXhbdTGZ+rtjLbXQRJ7R38a2RsG0m/yLt5bmM2mrrIsYRoz8Dc
GrhTxJYBTHBPHVf6d7aF26EtkMiCAY0J1kjzPHkoPGmDGdIEdxh7q3LKmb1FpZuvn1AuMpAt
qQZNtCWMiSNQavTXYGHTWhcSVYmMpYtIgmdZ0+BvjTvh0KdruefdaPwj4/rWVjRWUYoYr+Lb
KluTLdsQOAJJny/zXWHu9gQec/GqWK7zfxN8zW7bQQYnTnU8LaLo0m0GzbBu0NdIBMGabuPj
T/hGCq0FLOycMLaKNxIBbz009Io277hWQx6Yg58nqS24Qb64Bc2+qTbXAE5GgieBEc0NQYe/
oV5Dd4VSdCnZ4cPLlRu+whJdy422LR07Snzj56VG+0SNzn01P16VWbCqwgke6aqXtkT3XZfi
Pr1rKkF9Jbu7bjvE+Z/tUbbfQ72B+H6UMfZf3hcQ/wAU/wB6FYrYeIJ0FsnkDH5AVLzN0w8h
nEbetfiWfEwfeKHX8dmzgQDqIDfTRI0J/KgWJ2JiFDMyqqjUsbiAAcyS2gqnYHVroQc2oI0m
U6gjnI+dY77m0uwXw1sHT61ijeD2F1gJWNPY5c6AYK7ypq2dafJKtB1jSZP5b6yle50r7AHH
b0CyNKX8bag0e2hiZnhzpx+Ik0cedgXxuUHawNet9AtoW1wVpWuIGBeVzAETcYiRzj8qR+h
2Ctu1w3EVz10DCQNVlg+Zofm29m+wsqgMoMKZ375HESDoaZYtoYf2iYQgrctFWTOSMsGGu6
MB/EY0qfoHqVRWxLkDMeptEwJGaGI8WfQeCUsYfbHWW3t3UE8LgADgmd07jurW1tttdtWbFp
erFjKVVgzSyzBWzQJZd+7eTyr04xKWnbuN039r28Fefq8NbFx+0bzmSxedwHabUMiLRpypST
F3MdiVS5cgGT/KssQo3AwDHqT0pNvpN0kXE27avaAuq00wYHUx0g3CQCBqeGmsr0HusjqyEh
9wI39oFdPGCRW1aBk9NL9S1tp7Av3BbzLAYGUrGgExqeM1ldbylWKLSCDBrKykdYXxbA0QNZ
JPvNF0j+E6y+o9he23kuoHqYpfud8/xN8zTj0I/138Nv5tWNDYy2Y44YcatNc+NVcP3R9cKk
ffXMFfP0jDf9b6h2ntC1bUNccIG0Ezq3hAqN+76H/qFKfTE/cHzX5ius0aXxltEz9YmVp63
0JxPTGwhjNnPNfjupJN5vsr9pvZ4nmaHbLUG7BEjLc0/ketW4MmPb9PbUaW29SI+dDsb08a
CLVvXmxhfcNT7xSud9bFFQFljaW1Lt8/e0WHBdyA+W710vjRLtJCMdVAA5ECACPCgZpl2frh
tdYXSdY31kuAoMu4BppqweIItkk6DX/FJGy9/p+tN+E/0R8qnlyNvYXsa8T4yd/0l7Eb6N7R
73140BvfpTYGTy1dCmk3ddco08PoUF6WE/apm0yuvLV0/WiPRDvep/6GoZ0t/wDsf/mn50a5
FM6t2xdZQIzuQsz2TwB8PdU239kW1U5Lme7bUtdUcbYIExwyyPSfCl90431xFN0xNTaJ1LZ5
PE6cedDVMnu0KFZJBkbwfjwra90eLY35fLTRJeuY3DMSXtNnPei42/jvNZRzD2lyJ2R3V4Dk
Kylhwf/Z

-----px0JXq3DNsdR43veRZqHptH0--|

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.

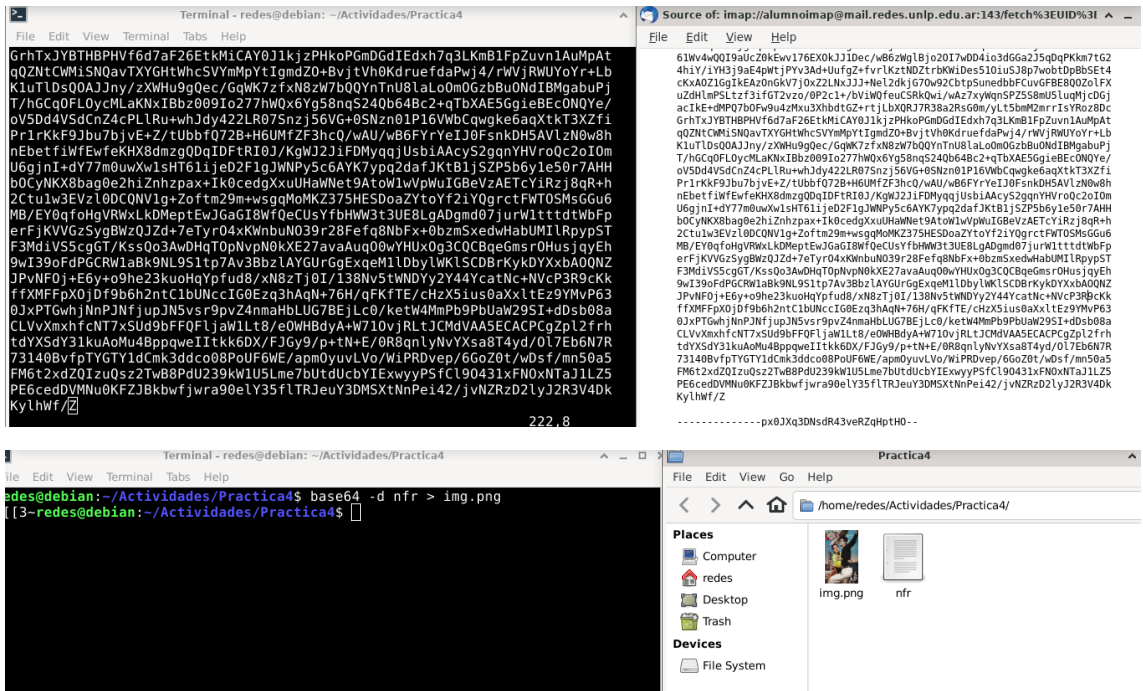
Para separar y marcar cada parte dentro de un mensaje MIME, se utiliza un identificador de límite llamado "boundary", que se establece en el encabezado "Content-Type".

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

- 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 receptiona dicho correo.

Envío

No.	Time	Source	Destination	Protocol	Length	Info
1	0.989898989	172.28.0.1	172.28.0.90	TCP	74	41828 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=320654134 TSecr=0 WS=128
2	0.990128070	172.28.0.90	172.28.0.1	TCP	74	25 → 41828 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=2781885441 TSecr=320654134 WS=128
3	0.990190297	172.28.0.1	172.28.0.90	TCP	66	41828 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=320654134 TSecr=2781885441
4	5.184231960	172.28.0.90	172.28.0.1	SMTP	126	S: 220 mail.redes.unlp.edu.ar ESMTP Postfix (Linux 4.01/GNU)
5	5.184297429	172.28.0.1	172.28.0.90	TCP	66	41828 → 25 [ACK] Seq=1 Ack=61 Win=64256 Len=0 TSval=320659318 TSecr=2781890625
6	5.187144171	172.28.0.1	172.28.0.90	SMTP	85	C: EHLO [172.28.0.1]
7	5.187177359	172.28.0.90	172.28.0.1	TCP	66	25 → 41828 [ACK] Seq=61 Ack=20 Win=65280 Len=0 TSval=2781890628 TSecr=320659321
8	5.186869127	172.28.0.90	172.28.0.1	SMTP	225	S: 250 mail.redes.unlp.edu.ar PIPELINING SIZE=1024000 VRCY ETNN STARTTLS ENHANCEDSTATUSCODES
9	5.187031250	172.28.0.1	172.28.0.90	TCP	66	41828 → 25 [ACK] Seq=20 Ack=220 Win=64128 Len=0 TSval=320659321 TSecr=2781890628
10	5.208971537	172.28.0.1	172.28.0.90	SMTP	131	C: MAIL FROM:<alumnoimap@redes.unlp.edu.ar> BODY=8BITIME SIZE=455
11	5.209009346	172.28.0.90	172.28.0.1	TCP	66	25 → 41828 [ACK] Seq=220 Ack=85 Win=65280 Len=0 TSval=2781890650 TSecr=320659343
12	5.213424048	172.28.0.90	172.28.0.1	SMTP	80	S: 250 2.1.0 Ok
13	5.213467324	172.28.0.1	172.28.0.90	TCP	66	41828 → 25 [ACK] Seq=85 Ack=234 Win=64128 Len=0 TSval=320659347 TSecr=2781890654
14	5.222271639	172.28.0.1	172.28.0.90	SMTP	185	C: RCPT TO:<alumnopop@redes.unlp.edu.ar>
15	5.222408947	172.28.0.90	172.28.0.1	TCP	66	25 → 41828 [ACK] Seq=234 Ack=124 Win=65280 Len=0 TSval=2781890663 TSecr=320659356
16	5.249894674	172.28.0.1	172.28.0.90	SMTP	80	S: 250 2.1.5 Ok
17	5.241025327	172.28.0.1	172.28.0.90	TCP	66	41828 → 25 [ACK] Seq=124 Ack=248 Win=64128 Len=0 TSval=320659375 TSecr=2781890682
18	5.261467642	172.28.0.1	172.28.0.90	SMTP	72	C: DATA
19	5.261728995	172.28.0.90	172.28.0.1	TCP	193	S: 354 End data with <CR><LF>.<CR><LF>
20	5.261762916	172.28.0.1	172.28.0.90	TCP	66	41828 → 25 [ACK] Seq=130 Ack=285 Win=64128 Len=0 TSval=320659396 TSecr=2781890703
21	5.275311814	172.28.0.1	172.28.0.90	SMTP	521	C: DATA fragment, 455 bytes
22	5.289364636	172.28.0.1	172.28.0.90	SMTP/I..	69	from: alumnoimap<alumnoimap@redes.unlp.edu.ar>, subject: probando ejer 4, (text/plain)
23	5.289664010	172.28.0.90	172.28.0.1	TCP	66	25 → 41828 [ACK] Seq=285 Ack=588 Win=64896 Len=0 TSval=2781890731 TSecr=320659409
24	5.302432346	172.28.0.1	172.28.0.90	SMTP	102	S: 250 2.0.0 Ok: queued as 7334760149
25	5.392488941	172.28.0.1	172.28.0.90	TCP	66	41828 → 25 [ACK] Seq=588 Ack=321 Win=64128 Len=0 TSval=320659436 TSecr=2781890743
26	5.315025734	172.28.0.1	172.28.0.90	SMTP	72	C: QUIT
29	5.325765452	172.28.0.90	172.28.0.1	SMTP	81	S: 221 2.0.0 Bye
30	5.325945092	172.28.0.90	172.28.0.1	TCP	66	25 → 41828 [FIN, ACK] Seq=336 Ack=594 Win=64896 Len=0 TSval=2781890767 TSecr=320659449
31	5.330156060	172.28.0.1	172.28.0.90	TCP	66	41828 → 25 [ACK] Seq=594 Ack=337 Win=64128 Len=0 TSval=320659478 TSecr=2781890780 TSecr=320659449
34	5.341787819	172.28.0.1	172.28.0.90	TCP	66	41828 → 25 [FIN, ACK] Seq=594 Ack=337 Win=64128 Len=0 TSval=320659476 TSecr=2781890767
35	5.341787819	172.28.0.1	172.28.0.90	TCP	66	25 → 41828 [ACK] Seq=337 Ack=595 Win=64896 Len=0 TSval=2781890783 TSecr=320659476

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	37.016771992	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=2781922459 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	37.044619727	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	37.045169040	172.28.0.90	172.28.0.1	POP/IMF	79	+			
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:	AGFsdWlub3BvcABhbHVtbn9wb3BwYXNz		
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	37.057921708	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	37.112269370	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	37.170800668	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
+
AGFsdWlub3BvcABhbHVtbn9wb3BwYXNz
+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 <alumnoimap@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: alumnoimap@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

- 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` recibe dicho correo.}**

Envío

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	5.050622948	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=8BITIME 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	5.072076327	172.28.0.90	172.28.0.1	SMTP	90 S: 250 2.1.0 Ok
19	5.075454789	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	5.095909416	172.28.0.1	172.28.0.90	SMTP	90 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	193 S: 354 End data with <CR><LF>.<CR><LF>
26	5.115090361	172.28.0.1	172.28.0.90	TCP	513 C: DATA fragment, 447 bytes
27	5.116876453	172.28.0.1	172.28.0.90	SMTP/L.	69 from: 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	192 S: 250 2.0.0 Ok: queued as B0FF160148
30	5.167546628	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=322607752 TSecr=2783839060

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	5.683001988	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...	503 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	5.750003979	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	5.832826406	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	5.883666974	172.28.0.1	172.28.0.90	IMAP	76 Request: 138 IDLE
63	5.883654930	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=77 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-b0fa7d78cdb@redes.unlp.edu.ar>
Date: Tue, 12 Sep 2023 17:53:09 -0300
To: alumnopop@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: 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 BDF100148
        for <alumnopop@redes.unlp.edu.ar>; Tue, 12 Sep 2023 20:53:14 +0000 (UTC)
Message-ID: <d5c7f272-efad-03ca-508d-b0fa7d78cdb@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: alumnopop@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

}
```

```

|
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

|
137 OK Fetch completed (0.001 + 0.000 secs).
138 IDLE
+ idling
* OK Still here
DONE
138 OK Idle completed (9.012 + 9.009 + 9.011 secs).
139 noop
139 OK NOOP completed (0.002 + 0.000 + 0.001 secs).
140 UID fetch 6:* (FLAGS)
* 3 FETCH (UID 5 FLAGS {\Recent})
140 OK Fetch completed (0.001 + 0.000 secs).
141 IDLE
+ idling
* OK Still here
DONE
141 OK Idle completed (120.104 + 120.102 + 120.103 secs).
142 noop
142 OK NOOP completed (0.001 + 0.000 secs).
143 UID fetch 6:* (FLAGS)
* 3 FETCH (UID 5 FLAGS {\Recent})
143 OK Fetch completed (0.001 + 0.000 secs).
144 IDLE
+ idling

```

Comandos:

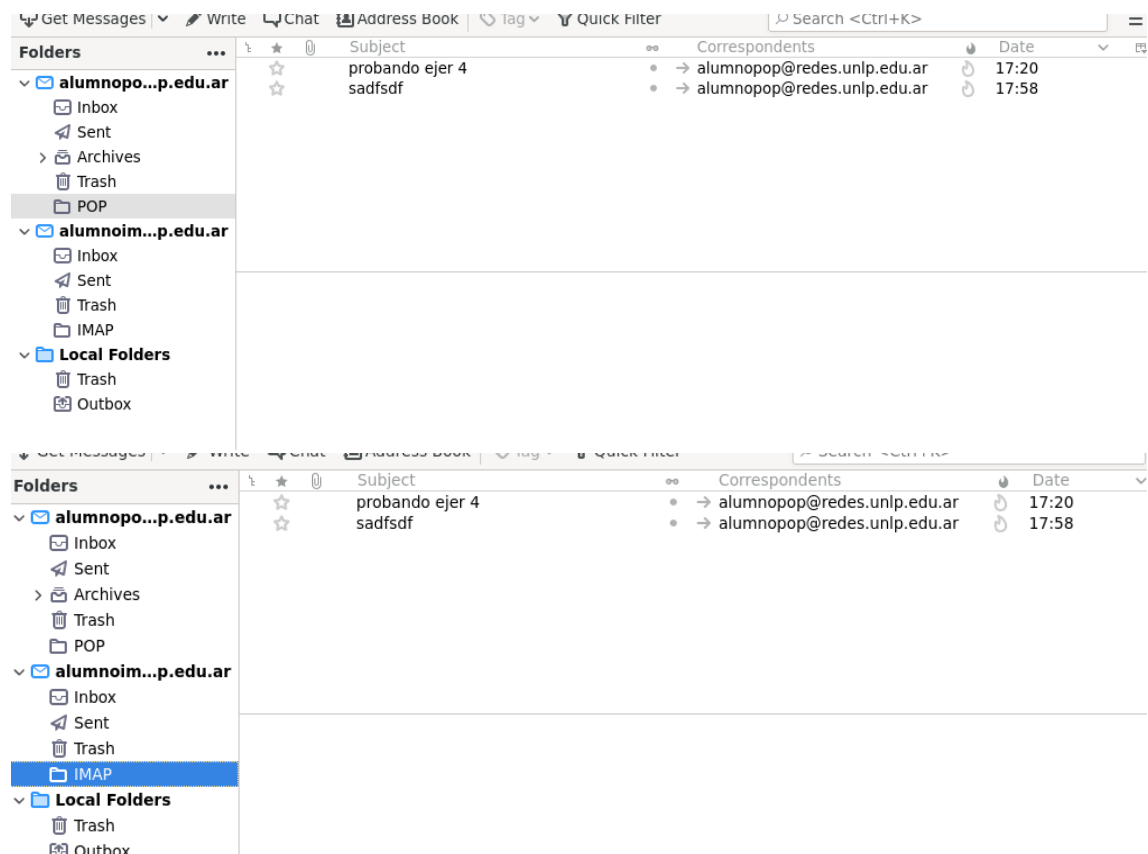
- DONE: El comando DONE se utiliza para indicar que se ha completado una transacción abierta en el servidor IMAP. Puede usarse para confirmar la finalización de una secuencia de comandos o transacción previamente iniciada.
- CHECK: El comando CHECK se utiliza para verificar la integridad de una carpeta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

- 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



- 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 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 leídos 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

En ambos casos, entre MUA-MSA si es posible enviar mas de un correo durante una misma conexión TCP. Entre MTA-MTA si se trata de destinatarios del mismo dominio se puede enviar en una misma conexión (aunque también podría haber conexiones distintas, verdaderamente depende si el MTA lo permite o como esta configurado). Si se trata de destinatarios de distintos dominios, siempre va a haber distintas conexiones, porque son dominios separados y responden a distintos servidores.

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

Sí, un MSA puede escuchar en un puerto TCP diferente a los convencionales. Hay que tener en cuenta que si se cambia el MSA hay que informar a todos los MUA del dominio que se cambió el puerto del MSA y estos tendrían que configurar el puerto.

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

Sí, es posible configurar un MTA para que escuche en un puerto TCP diferente al convencional. Sin embargo, hay que tener en cuenta que si se cambia el MTA se tendría que informar a todos los MTA de los otros dominios de dicho cambio, que a diferencia del cambio de puerto del MSA, es algo prácticamente imposible.

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?

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.

Sería 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
- correo.redes2022.com.ar 86400 IN A 203.0.113.8
- webmail.redes2022.com.ar 86400 IN CNAME correo.redes2022.com.ar
- 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 es necesario, porque al ser autoritativo para el dominio redes2022.com.ar no necesitaría resolver la petición consultando a otros servidores. No hay necesidad alguna de que haga recursión porque es el dueño de los dominios por los que se esta consultando. No debe delegar nada.

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

En los servidores DNS configuraría 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 actuaría como MUA, conectándose con el MSA usando el protocolo SMTP para pasarle el mail y que este se lo pase al MTA responsable de conectarse con el MTA receptor (siempre con el protocolo SMTP)

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 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.**

Se debería configurar en el registro SPF del servidor DNS con el dominio redes2022.com.ar y la dirección 203.0.113.111. No, esto no afectaría a los mails enviados desde la webmail, ya que esta estaría enviando los mails al MSA y el MSA recibe del MUA y se los pasa al MTA (con ip 203.0.113.111). Este MTA se lo pasara a cualquier otro MTA que reconocera como valido el mail proveniente de este (ya que tiene la ip que se encuentra en el SPF)

- 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 destinatario 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?**

Usará el protocolo SMTP. Se conectará con el MSA. El MUA debe conocer el puerto SMTP que se utilizará para la comunicación con el MSA. El puerto estándar para la comunicación con el MSA en la mayoría de los casos es el puerto 587 (SMTP Submission), pero también se podría usar el puerto 25 (SMTP) si está configurado de esa manera (u otro si no es ninguno de esos). En muchos casos, se requerirá autenticación del usuario antes de enviar el correo. Esto implica proporcionar un nombre de usuario y una contraseña válidos para el servidor MSA.

- 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 encolará 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-VERFY
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 agrega el MUA pero si falta lo agrega el MSA

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

Postfix es el servidor de correo electrónico que está siendo utilizado en la dirección "mail.redes.unlp.edu.ar" con la versión "Lihuen-4.01/GNU".

- 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
ZWNVZGUpPgpzdHJlYW0KeNqtWNtu20YQfddX8JECms3el5uX1E2TokGd0rVToIjzQJ00SoAiFV6c
uF/f2ZtESrIkI4IB7212dubsnNmhcLSicPTb7Jeb2ct3jEUJ0lKyJLq5jwgsYPivMEqkjJTQKGE6
ullGn+M36Sqdv6AqifPctRerqszSrLxlktVmSsUv3Mqbp2LxvWLqsj61sqUGcwRKZiM/vryonMC
```

- b. **Descargue de la plataforma la captura de tráfico smtp.pcapng 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 leído en la captura de tráfico?**

Porque este es encriptado ya que se usó el comando STARTTLS para comenzar una comunicación encriptada usando TLS.

- 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?**

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 775cbce5c3023956010000006501f3fd0d7f386c42b0388e (good)
;; QUESTION SECTION:
;info.unlp.edu.ar.                IN      TXT

;; ANSWER SECTION:
info.unlp.edu.ar.                300     IN      TXT     "MS=53F37089CAA39175A9111FF830E7F978A6B8036E"
info.unlp.edu.ar.                300     IN      TXT     "v=spf1 mx a:mailsecure.info.unlp.edu.ar 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:modle.linti.unlp.edu.ar ~all"
info.unlp.edu.ar.                300     IN      TXT     "google-site-verification=GQLud3qGeuqjRP0n-2INvgU0D-dkJUjvGrXICDqACgQ"
info.unlp.edu.ar.                300     IN      TXT     "google-site-verification=S5DXBH0Y_JiAEZ0VYUsukCNH35qBwL7KV1jwzZawRsE"
info.unlp.edu.ar.                300     IN      TXT     "google-site-verification=_KuE_Fg0H37zv4e70VJVyl_qGpamol5t_pMisXadMRU"

;; Query time: 80 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Wed Sep 13 14:40:13 -03 2023
```

El registro SPF determina qué servidores de correo y dominios tienen permitido enviar correo en nombre de un dominio. Aparecen muchos servidores autorizados porque son los distintos servidores y dominios de la facultad de informática.

Se utiliza "a:" para autorizar servidores por nombres de host, debes asegurarte de que estos nombres de host se resuelvan a direcciones IP correctas y actualizadas.

- 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"**

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

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 721cf611321e0348010000006501f60d1125557bf2c6cb0e (good)
;; QUESTION SECTION:
;outlook.com.                IN      TXT

;; ANSWER SECTION:
outlook.com.                300     IN      TXT      "v=spf1 include:spf-a.outlook.co
m include:spf-b.outlook.com ip4:157.55.9.128/25 include:spf.protection.outlook.c
om include:spf-a.hotmail.com include:_spf-ssg-b.microsoft.com include:_spf-ssg-c
.microsoft.com ~all"
outlook.com.                300     IN      TXT      "google-site-verification=0iLWhI
MhXEkeWwWfFU4ursTn-_0vo0jaA0Lr7Pg1sEM"
outlook.com.                300     IN      TXT      "google-site-verification=DC2uC-
T8kD33lINhNzfo0bNBw-vrCXs5BPF5BXY56g"

;; Query time: 952 msec
;; SERVER: 172.28.0.29#53(172.28.0.29)
;; WHEN: Wed Sep 13 14:49:01 -03 2023
;; MSG SIZE rcvd: 453
```

include:

spf-a.outlook.com
 spf-b.outlook.com
 spf.protection.outlook.com
 spf-a.hotmail.com
 _spf-ssg-b.microsoft.com
 _spf-ssg-c.microsoft.com

ip4:

157.55.9.128/25

"include" permiten especificar dominios o registros SPF externos que deben ser considerados como parte de la política SPF actual. Esto significa que los servidores autorizados para enviar correos en nombre del dominio se toman de esos registros externos.

Esto significa que los servidores autorizados para enviar correos en nombre de outlook.com se definen en los registros SPF de spf-a.outlook.com y spf-b.outlook.com. En lugar de enumerar todas las direcciones IP y servidores en el registro SPF de outlook.com, simplemente se hace referencia a estos registros externos para simplificar y mantener actualizada la política SPF.

```

redes@debian:~$ dig -t txt spf-a.outlook.com

;<>> DiG 9.16.27-Debian <>> -t txt spf-a.outlook.com
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20820
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 1232
; COOKIE: 9840ee35ffb9e3a501000000650234739abebd9a65fb8219 (good)
; QUESTION SECTION:
; spf-a.outlook.com.                IN      TXT

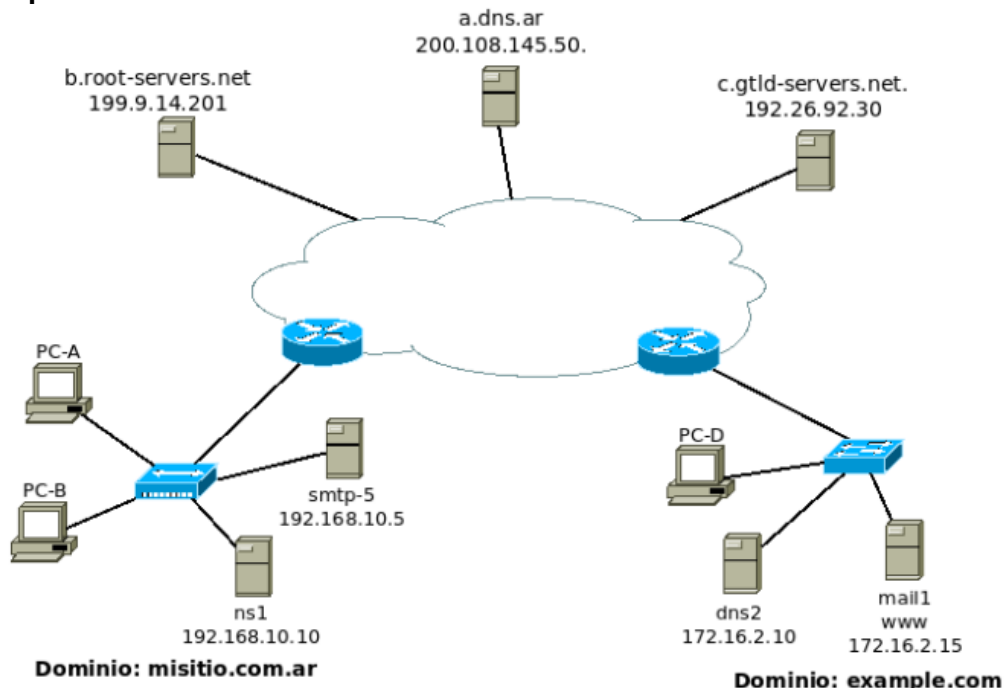
; ANSWER SECTION:
spf-a.outlook.com.      300     IN      TXT     "v=spf1 ip4:157.56.232.0/21 ip4:157.56.240.0/20 ip4:207.46.198.0/25 ip4:207.46.4.128/25 ip4:157.56.24.0/25 ip4:157.55.157.128/25 ip4:157.55.61.0/24 ip4:157.55.49.0/25 ip4:65.55.174.0/25 ip4:65.55.126.0/25 ip4:65.55.113.64/26 ip4:65.55.94.0/25 -all"

; Query time: 636 msec
; SERVER: 172.28.0.29#53(172.28.0.29)
; WHEN: Mon Jul 6 13:10:15 CEST 2003

```

“all” especifica una “falla suave” en la política SPF. Esto significa que, si el correo no proviene de ninguna de las fuentes autorizadas mencionadas anteriormente en la política SPF, el correo no se rechazará automáticamente, pero podría ser marcado como sospechoso o marcado de alguna otra manera por el destinatario.

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 sus 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?**

Si, es posible esto. Para que esto funcione correctamente, se debe asegurar que el servidor de correo y el servidor web estén configurados para escuchar en puertos diferentes. El protocolo SMTP se utiliza para el correo electrónico y generalmente se ejecuta en el puerto 25 o el puerto 587, mientras que HTTP utiliza el puerto 80 o el puerto 443 para conexiones seguras (HTTPS).

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

El MUA no consultara por ningún registro DNS, ya tiene configurado el servidor MSA al que debe enviar los correos electrónicos (se lo da el proveedor)

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

Este consultara el registro MX del dominio receptor (example.com)

- 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, seria necesario para obtener la IP de los nombres de servidores dados. Deberá preguntar por el registro A (siguiendo la prioridad)

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

El servidor DNS ns1 actúa como servidor DNS y realizar las consultas necesarias en nombre de SMTP-5

1. Consultará al root server más cercano (b.root-servers.net) y este proporcionará la dirección IP de un servidor DNS autoritativo para .com (c.gtld-servers.net)
2. Consultará con el servidor autoritativo de .com y este proporcionará la dirección IP de un servidor DNS autoritativo para example.com
3. ns1 consultará al servidor DNS autoritativo de example.com para obtener los registros MX específicos que indican los servidores de correo asociados con 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.** F → Los datos de la cabecera de SMTP deben ser analizados por el MSA para determinar si hay algún campo faltante que debe ser completado.
El servidor DNS no debe analizar los datos de la cabecera para responder a la consulta de los registros MX. Simplemente responde la consulta sin analizarlos.
- **Al ser recibidos por el servidor smtp-5 los datos agregados por el protocolo SMTP serán analizados por cada una de las capas inferiores.** V → En el modelo de capas de protocolo, cada capa es responsable de procesar y encapsular los datos antes de pasarlos a la capa inferior.
- **Cada protocolo de la capa de aplicación agregará una cabecera con información propia de ese protocolo.** F → No todos los protocolos de la capa de aplicación agregan 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 pueden ser analizadas y comprendidas por el protocolo SMTP o HTTP.** F → Los protocolos son independientes del resto. Cada protocolo de aplicación tiene su propia estructura de datos y cabeceras, y no están necesariamente diseñados para interoperar entre sí de manera directa.
- **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.** F → el protocolo HTTP provee la abstracción necesaria para que clientes que distintos sistemas operativos puedan acceder al mismo contenido sin problemas
- **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.** F → No, ya que el ns1 no es un servidor autoritativo de www.example.com, no lo va a tener en ningún registro y como www.example.com no es un subdominio de misitio.com.ar no va a poder delegar a otra zona. A su vez, ns1 no hace consultas recursivas fuera de misitio.com.ar (algo que se aclara en el enunciado). Si se tratara de un cliente web perteneciente al dominio, sí podría usarlo como servidor de DNS para resolver la consulta.

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

Ninguno. Es un protocolo distinto. Para ver el mail desde PC-D utilizara el protocolo POP3 o IMAP. DNS es un protocolo distinto para resolver nombres de dominios a IPs. El software de correo electrónico en PC-D se comunicaría directamente con el servidor de correo utilizando la dirección IP o el nombre de dominio previamente resuelto durante el proceso de configuración

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

Protocolos SMTP (25) para envío y POP3 (110) o IMAP (143) para recepción. Todos estos utilizan TCP.