

Práctica 4 - Redes y Comunicaciones

Ejercicios de la Práctica

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 el cliente y su servidor de correo, y entre servidores de correo 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.
 - Los protocolos que se utilizan para la recepción de mails son POP3 e IMAP.

POP3

- **POP3 (Post Office Protocol—Version 3)** es un protocolo de acceso a correo **simple**, por lo tanto su **funcionalidad es limitada**.
- POP3 se inicia cuando el agente de usuario (el cliente) abre una conexión TCP en el **puerto 110** al servidor de correo (el servidor). Una vez establecida la conexión TCP, POP3 pasa a través de tres fases:
 - **Autorización**
 - Durante esta fase el agente de usuario envía un nombre de usuario y una contraseña (en texto legible) para autenticar al usuario.
 - Tiene dos comandos principales: **user <nombreUsuario>** y **pass <contraseña>**.
 - **Transacción**
 - Durante esta fase el agente de usuario recupera los mensajes; también durante esta fase, el agente de usuario puede marcar los mensajes para borrado, eliminar las marcas de borrado y obtener estadísticas de correo.
 - Un agente de usuario que utilice POP3 suele ser configurado (por el usuario) para **“descargar y borrar”** o para **“descargar y guardar”**. La secuencia de comandos que ejecute un agente de usuario POP3 dependerá de en cuál de estos dos modos esté operando.
 - En el modo **descargar y borrar**, el agente de usuario ejecutará los comandos **list**, **retr** y **dele**. Tiene como **problema** que no guarda los mensajes en el servidor de correo después de que se hayan descargado.
 - En el modo **descargar y guardar**, el agente de usuario deja los mensajes en el servidor de correo después de que se hayan descargado.

■ Actualización

- Esta fase tiene lugar después de que el cliente haya ejecutado el comando **quit**, terminando la sesión POP3; en este instante, el servidor de correo borra los mensajes que han sido marcados para borrado.
- En una transacción POP3, el agente de usuario ejecuta comandos y el servidor devuelve para cada comando una respuesta. Existen dos posibles respuestas:
 - **+OK** (seguida en ocasiones por una serie de datos servidor-cliente), utilizada por el servidor para indicar que el comando anterior era correcto.
 - **-ERR**, utilizada por el servidor para indicar que había algún error en el comando anterior.
- **Durante una sesión POP3 entre un agente de usuario y el servidor de correo, el servidor POP3 mantiene cierta información de estado;** en concreto, mantiene la relación de los mensajes de usuario que han sido marcados para ser borrados. Sin embargo, **el servidor POP3 no conserva la información de estado de una sesión POP3 a otra.**

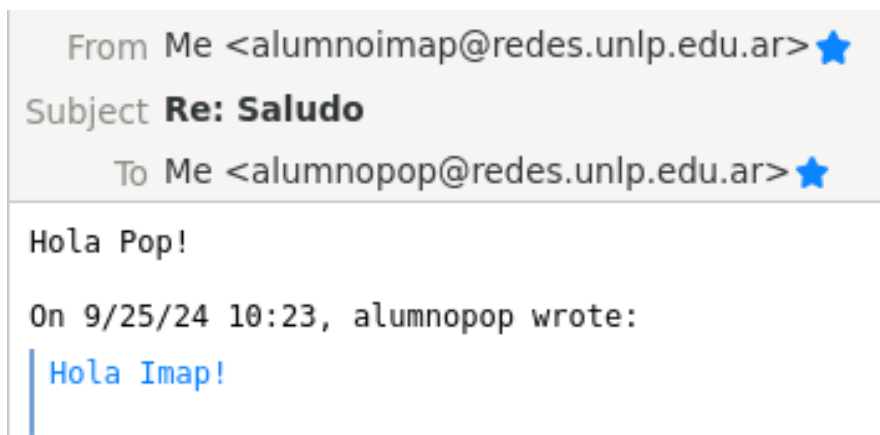
IMAP

- El protocolo **IMAP (Internet Mail Access Protocol)** es un protocolo de acceso a correo que ofrece muchas **más funcionalidades** que POP3 pero es más **complejo**.
- **Un servidor IMAP asociará cada mensaje con una carpeta;** cuando un mensaje llega al servidor, se asocia con la carpeta **INBOX (Bandeja de entrada)** del destinatario, el cual puede entonces pasar el mensaje a una nueva carpeta creada por el usuario, leer el mensaje, borrarlo, etc.
- Proporciona comandos para crear carpetas, mover mensajes entre carpetas, buscar mensajes que cumplan con ciertos criterios en carpetas remotas, etc.
- **Un servidor IMAP mantiene información acerca del estado a lo largo de las sesiones IMAP,** como por ejemplo, los nombres de las carpetas y los mensajes asociados con cada una de ellas.
- Dispone de comandos que permiten a un agente de usuario obtener partes componentes de los mensajes.

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.**



Correcto Funcionamiento

- 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**

352	230.679437375	172.28.0.99	172.28.0.1	SMTP	126 S: 220 mail.redes.unlp.edu.ar ESMTP Postfix (Lihuen-4.01/GNU)
354	230.769991940	172.28.0.1	172.28.0.99	SMTP	85 C: EHLO [172.28.0.1]
356	230.771936688	172.28.0.99	172.28.0.1	SMTP	225 S: 250-mail.redes.unlp.edu.ar PIPELINING SIZE 10240000 VRFY ETRN STARTTLS ENHANCEDSTATUSCODES 8BITMIM.
358	230.811776062	172.28.0.1	172.28.0.99	SMTP	130 C: MAIL FROM:<alumnopop@redes.unlp.edu.ar> BODY=8BITMIME SIZE=581
360	230.826224852	172.28.0.99	172.28.0.1	SMTP	80 S: 250 2.1.0 Ok
362	230.907706210	172.28.0.1	172.28.0.99	SMTP	106 C: RCPT TO:<alumnoimap@redes.unlp.edu.ar>
364	230.931943615	172.28.0.99	172.28.0.1	SMTP	80 S: 250 2.1.0 Ok
366	231.010813036	172.28.0.1	172.28.0.99	SMTP	72 C: DATA
367	231.017959539	172.28.0.99	172.28.0.1	SMTP	103 S: 354 End data with <CR><LF>.<CR><LF>
369	231.043415318	172.28.0.1	172.28.0.99	SMTP	647 C: DATA fragment, 581 bytes
370	231.077210260	172.28.0.1	172.28.0.99	SMTP/I...	69 from: alumnopop <alumnopop@redes.unlp.edu.ar>, subject: Consulta, (text/plain)
372	231.123984335	172.28.0.99	172.28.0.1	SMTP	102 S: 250 2.0.0 Ok: queued as 590B6691F7
374	231.141861262	172.28.0.1	172.28.0.99	SMTP	72 C: QUIT
375	231.146626208	172.28.0.99	172.28.0.1	SMTP	81 S: 221 2.0.0 Bye

Tráfico de red

- 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=581
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:
<65ede691-6100-5d63-7060-042b986a4879@redes.unlp.edu.ar>
Date: Wed, 25 Sep 2024 10:32:51 -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: Consulta
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit
Che Imap, no te parece medio raro que 200 pibes de una materia creen
cuentas con los mismos datos y hagan que nos comuniquemos como
boludos?
.
250 2.0.0 Ok: queued as 590B6601F7
QUIT
221 2.0.0 Bye
```

- c. Usando el cliente de correo Thunderbird del usuario alumnoimap@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.

From Me <alumnopop@redes.unlp.edu.ar> ★
Subject **Pitbull**
To Me <alumnoimap@redes.unlp.edu.ar> ★

DALE!

— pitbull.jpeg —



- i. **Verifique las fuentes del correo recibido para entender cómo 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 41C1760209
for <alumnoimap@redes.unlp.edu.ar>; Wed, 25 Sep 2024 13:41:24 +0000 (UTC)
Content-Type: multipart/mixed; boundary="-----w2xnKGdLK039CptB80rlbeCz"
Message-ID: <c4056c88-3989-6eb6-1aa0-56996ba5a9d2@redes.unlp.edu.ar>
Date: Wed, 25 Sep 2024 10:41:18 -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: Pitbull

This is a multi-part message in MIME format.

-----w2xnKGdLK039CptB80rlbeCz

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

Content-Transfer-Encoding: 7bit

DALE!

Content-Transfer-Encoding: base64

/9j/4AAQSkZJRgABAQAQAABAD/2wCEAAAGBxIREhUSEhIQRFRUWFRUFVFXUVRUQFxFYUG
BUWGBUVFRUYHSGGGBolGxUWITEhJSkrLi4uFx8zODMtNygtLisBCgoKDg0OGhAQGiOeHx0tL
S0rLS0tLS0tLS0tLS0tKy0tLS0tLS0tLS0tLS0tLS0tLSstLS0tLS0tLS0tLf/AABEIALEB
HQMBIgACEQEDEQH/xAAcAAEAQAUBAQAAAAAAAAAAAAAAAAAQIDBAHBQj/xABAEAAACAQ
IDBAcFBakDBQAAAAAAAQIDEQQSIQUGMUETIIIFhcYGhBzJSkbEjQsHRFBuzYnKCKrLwc+HxJ
DQ1osL/xAAZAQEAAwEBAAAAAAAAAAAAAAAAAQIEAwX/xAAmEQEBAAIBBAEEAgMAAAA
AAAAAAAAQIRAwQSITfBEylyUWGBBRRC/9oADAMBAAIRAxEAPwDuAAAAAAAAAAAFNSaim2
7Jatlrpm9e2c0uig+rH3u99ngimecxm1sMbldKtsbec24xdOL1Plhj2uDPhnXBvYi2YMs7btuxwk
mmww2k/iPRw+3HwdvoagrlcLoTksLxbb9Sx6kr8O7kJYpcn6mlUsXKPNmQsbfdmPro/19Nn
njeWZEUDpuD43XZ2/ka3+k3WrJp4n5CcUvHI6FqRkcVKPBlw1fd/aOWWRvSX15G0GvDLujLn
j20ABaqgAlAAAAAAKSohgQACEoIZLIJSoZBUUKDIABDUAAAAAAABg7axnQ0ZT52svFnM68
7s2rf3E26Onfk5P6L8TTYy1MPUZby039Nh9u1+EEXoxRbolyEjO1aMhblEvss1GBjzLeYuVCxJ
kJXqdUrjVdzGiy/TiXxcS49HC1mrM6Ds3EdJTjLnBXx5nOKJuO6Ve8ZQfJ3Rq4rq6Y+WeNtgA
BqZgAFQAAAAACGSAKQAKmDKSoghKgPZuyGBfAbdUAAAAAAABzfytfE2+GEV89fxPapnu
b+02sQ5dqj/al+B4VNnnC3516XT/jGZRkX3MxKbL8UcnddcI3MulpaJOljiWWi/Vkjy8dtGFPU
w7TBj4GTTh5mtfr9N9VN+CbpD2dKo0pOnJReuazS9S0xrllY9OJ7O7uOjSq2nJJNPi7cFc8Cp
WSZNXDZ4Tm+Ucq/mdtO+1/kdJdVxuMv8Abdl720XUyJSy3tmOt5l2FM4g05xUleLho1f7r4ea
OybHbdCk3x6OH9qO3DY3K2VHVDPjY43H5ZgANDCAAgAAAAAEMglkACCsgQspkUsqKU2
AvgAuqAAAAAAAAA1DfzB5sku2LXyd19TRY95v2921aOSULvNTkpN20stJa+DOY7z7co4WTTl
mnxyR1evBy5RMflJ3ZeG7gy7Z93h69OqQPTpHL6m/NW94whbsld/RouT9ovBLaNKIGxbZSX
yaKzgyXvU4Ol/palxWlcU5NNJK92mjIMt88RKWab5W+z+z8OHHvXON72bCjWgpN16rywcnH
LBjyipOKIJtu1+xFcuO4+18OaZ+mBj94lcZ1VThd6qOecrcckOfi9O81Lbe8MJ6UIstznV6832W
V8sflic8nbSkq9SMtGpNcLaLh/neX8LSLEVkvQqp5qmTpcqlD3MqlmzN24SXPmacOPGRkz5c
srphTx1SXvTk+6+nyWhcw833oooOT1MNQzvGMrIjDG1sm6+23TaVecnSfn3m402lrXbT4W7
OdCxeK6TB3pKd5da0oum/hj1XquLepz7ZeznFwfDr02v64nSaEbwd+z/cz+K0+rP4avgOOXua
9DsW7074ai/3F6aHIsDRetRaqcPw7lf8AI7Jsqqko049kl/Qt0s81f/lZS4zX7ZQANleWAAgAAA
AAEMglkACGSQyFkMpKmUki8ACyoAAAAAADn++Wyp03iaY60ZQhKKtfrZrv3dVf1HBdo4d
vrNtt9Zt6tt8Xc+oN6dgwxllLPpeDzRyznTTfwzytZovsZWra+wnGNvgbj5cYv5fRmbOdmW/wB
teGXfj5+HPZ03yLuCwOXOPSuap3WdwSc0ueVPS/ibZhdiO2Zrj9C/PYa+H8B9aH0ntWoYeh0
NTN0zrOSVO2VU1HS7nzB46l6TujOCpPo4uMXIST46U4KTfjJSfma5+pl8LWuvF2/zTZnr2Nhl
TgoLkvXmcuXk7o78PF214G9Ow41pud1GSi2ur77X3W1wfGz8jW9n7Gc9Yy04Pk/BnTcVh1Lij
wVgEq1tYrSS0v48n5lceS60tnxTu28jd7vLmZ2G2dGnLXyPcls6rb3o/lx4blblec2+5cH4ILbfdW
kk+GfgKEW4vzXyev5fM2XCWy2PGw1GMVoerhZHsenLJjbCwWerTprgpK65WvqdTRr+7uwY
0X0rm5uSzRVrKobW3fXsbAaeHDtjLz8vfZr4AAda4AAIAAAAABDIJAEMkhkLIZSVFIF4AF1Q
AAAAAAAAA0DfLd+Od1LPLJNq2lpCXHwdjfxyjcLGrBwlwfo+TKZ490dOPPtrimMoZ3eHBfds4v
8vUilhaz0St3y19Ofoc3tPCvD1ZRfBNr8jGeJsJBZq+XpYecWG8HGGjblJ6tlzB1FFlrDVbuU35GD
jMMpzZqUk072TtqRF/T2cXi4p5m0ktX5HkVtrU60YOGsnOOXSz0ert4XMHGJU1FlzO3Pvktn
YFUvEtrwr8tnVS6LKZYp1mXaMO2UTazYGZhuJh2MmjLU6xnydH2ZK9KH8K9EZRoCMbXnGp
h8PUdOrKk6IKdlJZ4uzi009HdLzOc7M9rm0aNTLiOiQJSyziKCpyi07NXiazT7jZhlumWePBxO

EDyd29v0sbS6Sno1pKL4xf4rvPWLKAAIAAAAAAKSopAEMkhhZDKGVspIF4AF1QAAAAAAA
AAad7QNkucOmgTq0l3cpeRzmOZ9Xmd1qQUk00mmrNPmjIG9mwJYSpeN+ik+pL4X8D/wA
1MvPx/wDUa+n5NfbXgVZuKtlk7Lkr/Qw5Y1X1ko9z4/I9OnjL6PSS9SjaGHhUWbKrruM0blwLSi
rTIWVteHF9ngY0MXTvpKpLXkm/VF14Ki+MI/RfLgXZuOkVlil4lvqOlkw8PinPSnTm++Tyr82e
ISzrWVvloTilaJm0k2ijlWVSqXLzrWsjAnPKYmK2goLNxfCK5tvgi8rly2/dirmryl8EMvn
Np2+UDT/AGxbn/aLH0I9Wo4xxEYr3ZaJVrdj0T77PmzdN18E6NFZ/wBpN55+L5eSsjy/adth
0sKqaduleV+HF/Sxp4/EZOWy5NK3Z2/VwtTNSIZq2j4SXOMI2Hct294KWMp5o9Wa96m3rHv
713nzZs+peRs2zNozoTjUpzcJLhb6Pu7jq5PoUGj7C9odGay4m1OXxq8oy8uMWbZgNqUK6vS
q05/wyTfmuKCGYAAAAAhkFTKQBDJIZCyGUITKQLwALqgAAAAAAAABqG9++sMK3Tp5ZVF
7zfuw7rc2BttWoopyk0kk223ZJLi2zj/tB9oKrQnRw9uiTs6j1dR/dyp8l31vxdjVd4d7sTi24Sq1
Mj4xvli/5VpY1TaOJv1VwXqyt8pbns1zq4aOlaWXPkDcfuybj3O56GHRJ6Mq9kFaNXDYihN
JpVFKz+GcUvrBmRt7d+dBuULuHJ/D3P8zLycXzGzi5dzVYmI2VGR40C2f0eJy1LuLWj5f5+Z
6GH3hS6k9JLj5FzE7Ug1fTkcZueGjXpwoQjwKp14xV7muVtsqK0Z5G0NqSb46f7MnHC2ozy
jY8ZtFRjmkz0dztlSrTWKrkYX7KD/vf4Hgs7Jlipxq1r9FH3Yv7/Zf936nTsMrJJHfHDTNn
yeNRnwZyn2v4+9anTT92Lk/ov/o6hOpZNnCN+MX0mNqv4bQXkrv1bOs9s9YeAr6nqxxSRrUJ
2MulXvoXVe3+nePzsWqW1KICpeM2lfRpu8X4mNSguN1p3pfUxsZjYz6kNe/8kEun7C9pmKp
pKbjWj2T4/wBS1+dzoE7u/eFxbUG+iqP7k3o3+7Lg/Q+asPiHE9LDY6z1dwh9Wg+fsDvXiYpJ
Yiu0uHXlp6nt4T2j4un70oVEuU46/NWYNOysg5/sn2qYadlXhOk/ij9pH818mbdgNv4Wv+Zr
0pN8syT+T1Bp6RDljUTbSabXFJp28ewlkJQyqkZRCc+AC6oAWsXil04SqS92EXJ+CV2BNavC
GspRiv3mo/U8/G7xYWI79aF+yLzv5RucR3k3oqYmU6kpaNpRjd2im0rLyZaoY1S5kbTp1rEb
/YaPuwqy/pivV39Dz6vtEf3cOvOp+UTns78TzcXtLpHj2gb7tv2i1nDLGMKbfOLcPfN8DIW
0ts56jjJtnvfnfUvYio5K9zXMTsvJyepAz6tfsMGRluozFIG7eyPaHR4103wq03H+aLzR9Mx
26dNNdtz5l2Rj3h69KsvuTjJ+HCX/q2fTGBrKcFJc0RVsWjb17jxq3qUerPjI5M5pjNIV6bc
ZpxabVndf8o+ip00aJ7RsdhcPTXTJSnL3l3n2y01UV2+RS4/p2mevbkiptcWbFu/uxOq1Ur
JqHGMHxI3y7u4xcBvDg4Vov9HquCespyjJx/ejBaPzbOsYOEJwjODUoySaa4NEduvZlnL6Ye
AwmVdh6lPQlUrEqmW8OaziqvVbfBK78j57xlfPkk6nxzLL5ts7hvviugwNefBuGSPjN5V9Th
BbFTJJVBIBKkSqqrqUvvadhTRVmLISnbvAyKhTGoQ53RabCds2li5R1TMv8AWLa14nj5ic4N
vVliwsXJtJNq/05mHnEZ2u/JeYntn3Z3mq4XFQRnLSSU1d2nG/Wi+3Q+nac1JKS1TSa8Hq
j4/w0tT6n3KxnTYDDVL3vRin4xWV+sRR7MillTKWRpK+AC6oa97Qqrhs7FNceia+bSfozYTy
t68LGrg8RTk1FSoz1eiXVbT+aA+Y8ViPs++8fqYix0lwbMetU6rXen6luo+ZVZsmzd4murPV
d5m4nJPrNNMTM3BY5xdmwhkzrvNKPJO3/JaxFK65CvNdJm+JJ+a0f4F2c9AI5EtCC5WWpa
CqJHe/ZrtXpsFSbd3FZJeMOr6pJ+ZwrBYSdaap04uUpcEvVt8ku06tutsuWCoun0jk5PNK2iTT
a0edtCmecxdelJuXp0HG7Yo0l1pq/wAK6z8NOHmca25sLEYyvPEVq0M03wSIJQj92Eb20S/E
3PJcs1aVuwzXmy+GydPjrZ5ajg90KcfelOT8oo2bdxywc3FTIKjN3dOWuR/FTfZ2r/HTafJQ
8b/hYs1KEpe9JL+FfiPqZftb6OGvToNNqSTVmnwZWoGh7A3heGxCw1d/ZVn9jN6ZKnDo5d0
uK7zfp1Ek23ZLVneeZtjymrpzX2zbSSjRwyerbqyXck4xv4tv+k5WetvVtj9MxVWv91yyw7qc
erD52v8AzM8k6xxtCCQEFxcFK4gXnlpbluQBnyLgi4Etk30RQ2TcDjpnfPYftPpMHUot60ql
0v3Zq/8AcpHAISN99km8IPB4t9NLLSqwySlyi7pwk+7ivMJj6lZDlpzUkpRaaamtU0+DTDI
SyAAXVDjXtk3tbqLB0Z9SNnVcX70r3UG+xa03a+46F7Q9qywuArVY00rRinwac5KOnfZs+Zs
di30Tk+LlqYw8W9WUXuiqoWoPT0IQIMquWyUwLyqvTuMiFYwmwpBLKrO5RhLKrONOHvSd
l+LfcuJZzm77g7laTxE173Vp37PvS8+HzK55ds2vx4d102XYOx6eGppMEs1utPnJ9/d3HqxRai
i+uwwd1telJJNRTUjoYtadkZDZh4qF2StKwv0httlYiUv2cZy70rJfzPQ9DlorkWquOSVkn
orW95dmYirSl7rtqoqXWTWujtx8ycXv+6my+ic/+pl9jL4svOq/GOni2ZG0drxjpe8vhWrfk
c4xDvOTtbrN24WuzVw+tVj6mau4qirklIHdKAAQlKxFFPFIYAEMgCopAApkSil8SpEiuLL1O
RjlUWB9Neyva8MRs6jGL61GKozXNOPuvwcbeptx8/exreD9HxipSdqelXRu/BTV3TfzvH+Y+
gSqWQAC6HPPbj/4+P+tD+2R8+TAIqYtSLa5kgHCAIQBJAAB8DsmY/wBhS/04f2oAzdT6jV0v

us6HBEyAM0bVE+JjVyQTUMXFcDxcV+ABOKawdzffq/xGq7z/APcz8QDRx/my8/4MFAA0MQ
AALdPiytgAQAAJIAAtriVoAmCSUASPQ2X+0p/xx+qPrWlwXgvoAUqX/9k=

-----w2xnKGdLK039CptB80rlbeCz--

- La extensión del formato de los mensajes de correo MIME (Multipurpose Internet Mail Extensions) permite que los correos electrónicos puedan contener más que solo texto simple, como imágenes, archivos adjuntos, videos, y diferentes tipos de contenido multimedia o estructuras complejas. MIME hace uso del header "**Content-Type: multipart/mixed**" que indica que el mensaje contiene diferentes tipos de contenido combinados en una única estructura, y que esos contenidos pueden ser de naturaleza distinta, como texto, imágenes, archivos adjuntos, etc.
 - El header **Content-Type** es usado para especificar el tipo de contenido del cuerpo del mensaje en un correo electrónico o en una solicitud HTTP. En este caso, **multipart/mixed** es uno de los varios tipos de contenido posibles.
 - **Multipart** significa que el correo está dividido en múltiples partes. Cada parte tiene su propio tipo de contenido (por ejemplo, texto, imagen, archivo adjunto, etc.). Este tipo de mensajes suele incluir varias secciones separadas por un delimitador.
 - **Mixed** especifica que el mensaje puede contener diferentes tipos de contenido que no están necesariamente relacionados entre sí.

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

- **ESTE NO LO PUDE HACER PERO LOS PASOS A SEGUIR SERÍAN:**
 - Copiar el source de la imagen en un archivo txt por ejemplo.
 - Usar el comando **base64 -d imagen_base64.txt > imagen.jpg** así de esta forma con base64 podemos decodificar la imagen y dejarla en un archivo .jpg.

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.**

237	73.493610070	172.28.0.90	172.28.0.1	SMTP	126 S: 220 mail.redes.unlp.edu.ar ESMTP Postfix (Lihuen-4.01/GNU)
239	73.507102165	172.28.0.1	172.28.0.90	SMTP	85 C: EHLO [172.28.0.1]
241	73.511775510	172.28.0.90	172.28.0.1	SMTP	225 S: 250-mail.redes.unlp.edu.ar PIPELINING SIZE 10240000 VRFY ETRN STARTTLS ENHANCEDSTATUSCODES 8BITMIM...
243	73.538629368	172.28.0.1	172.28.0.90	SMTP	131 C: MAIL FROM:<alumnoimap@redes.unlp.edu.ar> BODY=8BITMIME SIZE=490
245	73.581884888	172.28.0.90	172.28.0.1	SMTP	80 S: 250 2.1.0 Ok
247	73.593970976	172.28.0.1	172.28.0.90	SMTP	105 C: RCPT TO:<alumnoimap@redes.unlp.edu.ar>
249	73.652123962	172.28.0.90	172.28.0.1	SMTP	80 S: 250 2.1.5 Ok
250	73.654201952	172.28.0.1	172.28.0.90	SMTP	72 C: DATA
252	73.655015235	172.28.0.90	172.28.0.1	SMTP	103 S: 354 End data with <CR><LF>.<CR><LF>
253	73.661816293	172.28.0.1	172.28.0.90	SMTP	556 C: DATA fragment, 490 bytes
255	73.702830986	172.28.0.1	172.28.0.90	SMTP/I	60 from: alumnoimap <alumnoimap@redes.unlp.edu.ar>, subject: test, (text/plain)
257	73.747343141	172.28.0.90	172.28.0.1	SMTP	102 S: 250 2.0.0 Ok: queued as 38C5760184
258	73.768487936	172.28.0.1	172.28.0.90	SMTP	72 C: QUIT
261	73.781128704	172.28.0.90	172.28.0.1	SMTP	81 S: 221 2.0.0 Bye

Envío

10	3.248966821	172.28.0.90	172.28.0.1	POP	86 S: +OK Dovecot ready.
12	3.249841537	172.28.0.1	172.28.0.90	POP	72 C: CAPA
14	3.250793087	172.28.0.90	172.28.0.1	POP	155 S: +OK
16	3.253444537	172.28.0.1	172.28.0.90	POP	78 C: AUTH PLAIN
18	3.258920173	172.28.0.90	172.28.0.1	POP/IMF	70 +
20	3.260949067	172.28.0.1	172.28.0.90	POP	100 C: AGFsdW1ub3BvcABhbHVtbn9wb3BwYXNz
22	3.294682886	172.28.0.90	172.28.0.1	POP	82 S: +OK Logged in.
24	3.303769956	172.28.0.1	172.28.0.90	POP	72 C: STAT
26	3.307190106	172.28.0.90	172.28.0.1	POP	78 S: +OK 2 1775
27	3.326383675	172.28.0.1	172.28.0.90	POP	72 C: LIST
29	3.331849629	172.28.0.90	172.28.0.1	POP	100 S: +OK 2 messages:
30	3.343161637	172.28.0.1	172.28.0.90	POP	72 C: UIDL
32	3.344074677	172.28.0.90	172.28.0.1	POP	114 S: +OK
34	3.402255316	172.28.0.1	172.28.0.90	POP	72 C: QUIT
36	3.405929417	172.28.0.90	172.28.0.1	POP	84 S: +OK Logging out.

Recepción

- 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

+

AGFsdW1ub3BvcABhbHVtbn9wb3BwYXNz

+OK Logged in.

STAT

+OK 3 2587

LIST

+OK 3 messages:

1 979

2 796
3 812
.
UIDL
+OK
1 0000000356eaa394
2 0000000456eaa394
3 0000000556eaa394
.
RETR 3
+OK 812 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 3BC5760184
for <alumnopop@redes.unlp.edu.ar>; Sat, 28 Sep 2024 16:06:24 +0000 (UTC)
Message-ID: <6c6e6aa7-ab04-b73c-4632-e88228f8edd7@redes.unlp.edu.ar>
Date: Sat, 28 Sep 2024 13:06:18 -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: test
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 8bit
este es un mensaje de test para capturar tr..fico smtp
.
QUIT
+OK Logging out.

- Comandos Utilizados
 - CAPA (Capabilities)
 - Este comando permite al **cliente** solicitar al servidor una **lista de sus capacidades**. Esto le dice al cliente qué características y extensiones admite el servidor, de manera que el cliente puede ajustar su comportamiento en función de las capacidades ofrecidas.
 - La lista de capacidades que devolvió el servidor fue:
 - **TOP** → Permite recuperar solo las cabeceras y una parte del cuerpo del mensaje.
 - **UIDL** → Proporciona un identificador único para cada mensaje en la bandeja de entrada, útil para identificar correos de manera única.

- **RESP-CODES** → Indica que el servidor puede enviar códigos de respuesta en algunas circunstancias especiales.
 - **PIPELINING** → Permite enviar múltiples comandos sin esperar una respuesta intermedia del servidor, optimizando la comunicación.
 - **AUTH-RESP-CODE** → Indica que el servidor soporta códigos de respuesta para la autenticación.
 - **STLS** → Soporta la actualización de la conexión a una conexión segura (STARTTLS) si es necesario.
 - **USER** → Indica que el servidor permite autenticación con el comando USER.
 - **SASL PLAIN** → Indica soporte para autenticación SASL usando el mecanismo PLAIN (autenticación en texto plano).
- **AUTH PLAIN**
 - Este comando inicia el **proceso de autenticación** utilizando el método **PLAIN del protocolo SASL (Simple Authentication and Security Layer)**. En el método PLAIN, el cliente envía el **nombre de usuario y la contraseña codificados en Base64**. Aunque el método es sencillo, es **inseguro** si no se utiliza una conexión cifrada (por ejemplo, con STARTTLS o SSL/TLS), ya que **las credenciales son transmitidas en texto plano**.
 - El **servidor** responde con un **“+”**, esto significa que está listo para recibir las credenciales del cliente.
 - El **cliente** luego le envía la cadena codificada **AGFsdW1ub3BvcABhbHVtbm9wb3BwYXNz**. Que luego de decodificar se transforma en **alumnopop\alumnopoppass**.
 - El **servidor** envía como respuesta **+OK Logged in**, confirmando de esta forma que la autenticación fue exitosa.
 - **STAT**
 - Este comando solicita al **servidor** el estado general de la bandeja de entrada, específicamente el **número de mensajes que contiene** y el **tamaño total de todos esos mensajes en octetos (bytes)**.
 - El **servidor** devuelve la información con el formato **+OK <número de mensajes> <tamaño total>**, en este caso **+OK 3 2587**.
 - **LIST**
 - Este comando proporciona una **lista de todos los mensajes en la bandeja de entrada, junto con su tamaño individual en octetos**. Esto permite al cliente identificar qué mensajes están presentes en el buzón y cuál es el tamaño de cada uno.
 - El **servidor** responde con la lista de mensajes con el formato **<número de mensaje> <tamaño total>**.
 - **UIDL (Unique Identifier Listing)**

- Este comando es utilizado para obtener un **identificador único para cada mensaje en la bandeja de entrada**.
- El **servidor** devuelve la lista de identificadores únicos para cada mensaje en el formato **<número de mensaje> <UID>**.
- **RETR 3 (RETR <número de mensajes>)**
 - Este comando permite al **cliente** solicitar la **descarga completa de un mensaje específico desde el servidor**. En este caso, el cliente está solicitando el mensaje número 3. El **servidor** devolverá el **contenido completo del mensaje, incluidos los encabezados y el cuerpo**.
- **QUIT**
 - Este comando 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 un correo a **alumnoimap@redes.unlp.edu.ar** y mientras **alumnoimap@redes.unlp.edu.ar** recibe dicho correo.

175	65.488139258	172.28.0.98	172.28.0.1	SMTP	126 S: 220 mail.redes.unlp.edu.ar ESMTP Postfix (Lihuen-4.01/GNU)
177	65.539764789	172.28.0.1	172.28.0.98	SMTP	85 C: EHLO [172.28.0.1]
179	65.541496339	172.28.0.98	172.28.0.1	SMTP	225 S: 250-mail.redes.unlp.edu.ar PIPELINING SIZE 1024000 VRFY ETRN STARTTLS ENHANCEDSTATUSCODES 8BITMIME
181	65.581415609	172.28.0.1	172.28.0.98	SMTP	130 C: MAIL FROM:<alumnopop@redes.unlp.edu.ar> BODY=8BITMIME SIZE=555
183	65.596278663	172.28.0.98	172.28.0.1	SMTP	80 S: 250 2.1.0 Ok
185	65.615735713	172.28.0.1	172.28.0.98	SMTP	100 C: RCPT TO:<alumnoimap@redes.unlp.edu.ar>
187	65.642853928	172.28.0.98	172.28.0.1	SMTP	80 S: 250 2.1.5 Ok
189	65.661482045	172.28.0.1	172.28.0.98	SMTP	72 C: DATA
190	65.663568515	172.28.0.98	172.28.0.1	SMTP	103 S: 354 End data with <CR><LF>.<CR><LF>
192	65.684288452	172.28.0.1	172.28.0.98	SMTP	621 C: DATA fragment, 555 bytes
193	65.698073525	172.28.0.1	172.28.0.98	SMTP/I..	60 from: alumnopop <alumnopop@redes.unlp.edu.ar>, subject: Segundo test, (text/plain)
195	65.727076365	172.28.0.98	172.28.0.1	SMTP	102 S: 250 2.0.0 Ok: queued as 70BD7601D4
196	65.768363735	172.28.0.1	172.28.0.98	SMTP	72 C: QUIT
197	65.773749552	172.28.0.98	172.28.0.1	SMTP	81 S: 221 2.0.0 Bye

Envío

203	66.309150641	172.28.0.98	172.28.0.1	IMAP	90 [TCP ACKed unseen segment] Response: * 4 EXISTS
205	66.347960005	172.28.0.1	172.28.0.98	IMAP	72 Request: DONE
207	66.548677602	172.28.0.98	172.28.0.1	IMAP	125 Response: 191 OK Idle completed (102.843 + 102.788 + 102.842 secs).
209	66.554477460	172.28.0.1	172.28.0.98	IMAP	76 Request: 192 noop
211	66.555931964	172.28.0.98	172.28.0.1	IMAP	111 Response: 192 OK NOOP completed (0.001 + 0.000 secs).
213	66.556793839	172.28.0.1	172.28.0.98	IMAP	93 Request: 193 UID fetch 6:* (FLAGS)
215	66.558216492	172.28.0.98	172.28.0.1	IMAP	147 Response: 193 OK Fetch completed (0.001 + 0.000 secs).
217	66.560818816	172.28.0.1	172.28.0.98	IMAP	249 Request: 194 UID fetch 6 (UID RFC822.SIZE FLAGS BODY.PEEK[HEADER.FIELDS (From To Cc Bcc Subject Date Message-ID Pri
219	66.576815297	172.28.0.98	172.28.0.1	IMAP/I..	587 from: alumnopop <alumnopop@redes.unlp.edu.ar>, subject: Segundo test, (text/plain)
221	66.712052321	172.28.0.1	172.28.0.98	IMAP	113 Request: 195 UID fetch 6 (UID RFC822.SIZE BODY.PEEK[])
223	66.716151335	172.28.0.98	172.28.0.1	IMAP/I..	1049 from: alumnopop <alumnopop@redes.unlp.edu.ar>, subject: Segundo test, (text/plain)
225	66.837336162	172.28.0.1	172.28.0.98	IMAP	179 Request: 196 UID fetch 6 (UID BODY.PEEK[HEADER.FIELDS (Content-Type Content-Transfer-Encoding)]) BODY.PEEK[TEXT]<0.2
227	66.843764662	172.28.0.98	172.28.0.1	IMAP/I..	436 (text/plain)
229	66.931351666	172.28.0.1	172.28.0.98	IMAP	76 Request: 197 IDLE
231	66.935474192	172.28.0.98	172.28.0.1	IMAP	76 Response: + idling
250	83.952994869	172.28.0.1	172.28.0.98	IMAP	83 Response: * OK Still here
261	83.958479713	172.28.0.98	172.28.0.1	IMAP	72 Request: DONE
263	83.960267529	172.28.0.1	172.28.0.98	IMAP	122 Response: 197 OK Idle completed (17.028 + 17.022 + 17.027 secs).
265	83.963592994	172.28.0.98	172.28.0.1	IMAP	76 Request: 198 noop
267	83.969245908	172.28.0.1	172.28.0.98	IMAP	119 Response: 198 OK NOOP completed (0.005 + 0.000 + 0.004 secs).
269	83.973125933	172.28.0.98	172.28.0.1	IMAP	93 Request: 199 UID fetch 7:* (FLAGS)
271	83.974738333	172.28.0.1	172.28.0.98	IMAP	147 Response: 199 OK Fetch completed (0.001 + 0.000 secs).
273	84.099868400	172.28.0.98	172.28.0.1	IMAP	76 Request: 200 IDLE
275	84.103169757	172.28.0.1	172.28.0.98	IMAP	76 Response: + idling
277	91.293335518	172.28.0.98	172.28.0.1	IMAP	72 Request: DONE
279	91.294880235	172.28.0.1	172.28.0.98	IMAP	119 Response: 200 OK Idle completed (7.194 + 7.191 + 7.193 secs).
281	91.297053014	172.28.0.98	172.28.0.1	IMAP	76 Request: 201 noop
283	91.299222224	172.28.0.1	172.28.0.98	IMAP	111 Response: 201 OK NOOP completed (0.001 + 0.000 secs).
285	91.301198935	172.28.0.98	172.28.0.1	IMAP	93 Request: 202 UID fetch 7:* (FLAGS)
287	91.303515960	172.28.0.1	172.28.0.98	IMAP	147 Response: 202 OK Fetch completed (0.001 + 0.000 secs).

Recepción

- 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.

* 4 EXISTS

* 1 RECENT

[1 bytes missing in capture file].DONE

191 OK Idle completed (102.843 + 102.788 + 102.842 secs).

192 noop

192 OK NOOP completed (0.001 + 0.000 secs).

193 UID fetch 6:* (FLAGS)

* 4 FETCH (UID 6 FLAGS (\Recent))

193 OK Fetch completed (0.001 + 0.000 secs).

194 UID fetch 6 (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)])

* 4 FETCH (UID 6 RFC822.SIZE 879 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)] {271}

Message-ID: <3c8d0391-02c0-5a26-eed0-478fd251fb2d@redes.unlp.edu.ar>

Date: Sat, 28 Sep 2024 15:09:01 -0300

To: alumnoimap@redes.unlp.edu.ar

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

Subject: Segundo test

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

)

194 OK Fetch completed (0.016 + 0.000 + 0.015 secs).

195 UID fetch 6 (UID RFC822.SIZE BODY.PEEK[])

* 4 FETCH (UID 6 RFC822.SIZE 879 BODY[] {879}

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 7DBD7601D4

for <alumnoimap@redes.unlp.edu.ar>; Sat, 28 Sep 2024 18:09:06 +0000 (UTC)

Message-ID: <3c8d0391-02c0-5a26-eed0-478fd251fb2d@redes.unlp.edu.ar>

Date: Sat, 28 Sep 2024 15:09:01 -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: Segundo test

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

Content-Transfer-Encoding: 7bit

Este mensaje es para testear el flujo de mensajes de un POP a un IMAP para luego analizar los comandos de IMAP

)

195 OK Fetch completed (0.002 + 0.000 + 0.001 secs).

196 UID fetch 6 (UID BODY.PEEK[HEADER.FIELDS (Content-Type Content-Transfer-Encoding)] BODY.PEEK[TEXT]<0.2048>)

* 4 FETCH (UID 6 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> {116}

Este mensaje es para testear el flujo de mensajes de un POP a un IMAP para luego analizar los comandos de IMAP

)

196 OK Fetch completed (0.006 + 0.000 + 0.005 secs).

197 IDLE

+ idling

* OK Still here

DONE

197 OK Idle completed (17.028 + 17.022 + 17.027 secs).

198 noop

198 OK NOOP completed (0.005 + 0.000 + 0.004 secs).

199 UID fetch 7:* (FLAGS)

* 4 FETCH (UID 6 FLAGS (\Recent))

199 OK Fetch completed (0.001 + 0.000 secs).

200 IDLE

+ idling

DONE

200 OK Idle completed (7.194 + 7.191 + 7.193 secs).

201 noop

201 OK NOOP completed (0.001 + 0.000 secs).

202 UID fetch 7:* (FLAGS)

* 4 FETCH (UID 6 FLAGS (\Recent))

202 OK Fetch completed (0.001 + 0.000 secs).

203 IDLE

+ idling

- Comandos Utilizados
 - <número de mensajes> RECENT
 - El **servidor** informa cuántos mensajes nuevos han llegado desde la última vez que se revisó la carpeta.
 - NOOP (No Operation)
 - Este comando es utilizado por el **cliente** para **mantener la conexión activa con el servidor IMAP sin realizar ninguna acción específica**. Es útil para evitar que el servidor cierre la conexión por **inactividad**.
 - El **servidor** responde de la forma **192 OK NOOP completed (0.001 + 0.00 secs)** indicando que la operación NOOP se completó correctamente.

- **UID FETCH**

- Este comando permite al **cliente** solicitar **información detallada sobre un mensaje o un conjunto de mensajes, identificados por su UID (Unique Identifier)**. Es un comando versátil que se utiliza para obtener las **cabeceras, cuerpo del mensaje y otros detalles específicos**.
- En una **primera** ejecución el **cliente** hace:
 - **193 UID fetch 6:* (FLAGS)**
solicitando sobre los flags de todos los mensajes desde el UID 6 hasta el último (*). El **servidor** responde:
 - *** 4 FETCH (UID 6 FLAGS (\Recent))**
193 OK Fetch completed (0.001 + 0.000 secs).
indicando que el mensaje con UID 6 tiene el flag **\Recent**, es decir, es un mensaje reciente que no ha sido leído aún.
- En una **segunda** ejecución el **cliente** hace:
 - **194 UID fetch 6 (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)])**
solicitando **información más detallada** del mensaje con UID 6, el cliente solicita el **tamaño del mensaje, los flags** y los **campos de cabecera específicos**, como From, To, Subject, Date, etc. El **servidor** responde:
 - *** 4 FETCH (UID 6 RFC822.SIZE 879 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)] {271})**
Message-ID:
<3c8d0391-02c0-5a26-eed0-478fd251fb2d@redes.unlp.edu.ar>
Date: Sat, 28 Sep 2024 15:09:01 -0300
To: alumnoimap@redes.unlp.edu.ar
From: alumnopop <alumnopop@redes.unlp.edu.ar>
Subject: Segundo test
Content-Type: text/plain; charset=UTF-8; format=flowed)
194 OK Fetch completed (0.016 + 0.000 + 0.015 secs).
indicando que el mensaje con UID 6 tiene el flag **\Recent** y que el tamaño del mensaje es de 879 octetos. A su vez, retorna los campos cabecera solicitados con sus respectivos valores.

- **BODY.PEEK**

- Este comando permite al **cliente** **descargar una parte del cuerpo del mensaje sin marcarlo como leído**. En este caso, el cliente solicita los campos del header y parte del contenido del

cuerpo del mensaje, pero sin cambiar el estado de lectura, haciendo **195 UID fetch 6 (UID RFC822.SIZE BODY.PEEK[])**.

- El **servidor** devuelve el contenido completo del cuerpo del mensaje con UID 6. Incluyendo toda la información de la cabecera y el cuerpo.
 - *** 4 FETCH (UID 6 RFC822.SIZE 879 BODY[] {879}**
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 7DBD7601D4
for <alumnoimap@redes.unlp.edu.ar>; Sat, 28 Sep 2024 18:09:06 +0000 (UTC)
Message-ID:
<3c8d0391-02c0-5a26-eed0-478fd251fb2d@redes.unlp.edu.ar>
Date: Sat, 28 Sep 2024 15:09:01 -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: Segundo test
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit
Este mensaje es para testear el flujo de mensajes de un POP a un IMAP para luego analizar los comandos de IMAP
)
195 OK Fetch completed (0.002 + 0.000 + 0.001 secs).

○ **IDLE**

- Este comando permite al **cliente** permanecer en **estado de espera** sin cerrar la conexión. Durante este estado, el **servidor** puede notificar al cliente de cualquier cambio, como la llegada de nuevos correos.
 - **197 IDLE**
+ idling
- El **servidor** confirma que la conexión está ahora en modo IDLE, esperando notificaciones del **servidor** sin que el **cliente** tenga que enviar más comandos.

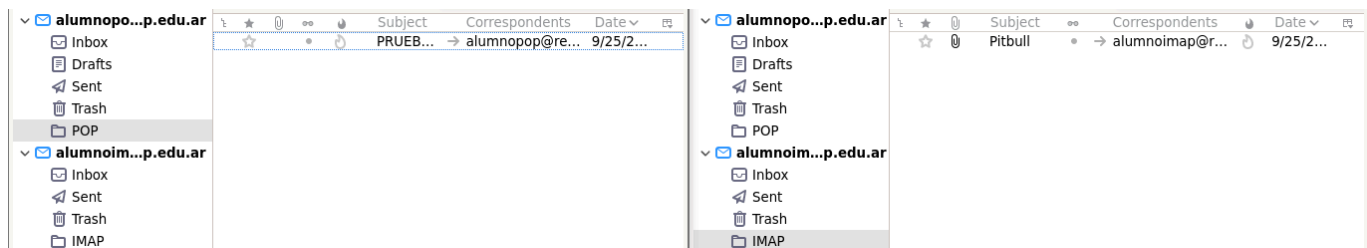
○ **DONE**

- El **cliente** envía DONE para salir del estado de IDLE.

- El **servidor** confirma que el modo IDLE se ha completado y la conexión sigue activa.
 - **197 OK Idle completed (17.028 + 17.022 + 17.027 secs).**
- **FETCH (UID <número> FLAGS (<flags>))**
 - Este comando solicita las **flags** de un **mensaje específico** o de un conjunto de mensajes.
 - Si es nuevo **\Recent**.
 - Si ya fue leído **\Seen**.
 - Si fue marcado para eliminación **\Deleted**.
 - etc.

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



- b. Cierre la sesión de la máquina virtual del usuario **redes** e ingrese nuevamente identificándose 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**. Responda:

- i. ¿Qué correos ve en el buzón de entrada de ambas cuentas? ¿Están marcados como leídos o como no leídos? ¿Por qué?
- En la cuenta del **alumnopop** veo los mensajes recibidos y están **marcados como no leídos**. En la cuenta del **alumnoimap** veo los mensajes recibidos y están **marcados como leídos**. Esto se debe a que:
 - Con **POP** el estado de los mensajes generalmente se maneja localmente en el cliente, entonces, cuando se accede a una cuenta desde otro cliente o dispositivo, ese cliente descargará los mensajes como si fueran nuevos. Los cambios realizados en un cliente **POP** no se sincronizan con el servidor.

- Con **IMAP** se trabaja directamente con los mensajes en el servidor de correo, por lo tanto, los cambios que se realicen en un cliente de correo se sincronizarán automáticamente en el servidor haciendo que esos cambios se vean reflejados para todos los clientes.

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

- La carpeta de **POP** no está pero la de **IMAP** sí. Esto se debe a que el protocolo **POP** no está diseñado para sincronizar la estructura de carpetas ni los estados de los mensajes con el servidor. Su función principal es descargar los mensajes del inbox del servidor y almacenarlos localmente en el dispositivo del cliente. En el caso de **IMAP** las carpetas y los estados de los mensajes se ven almacenados y sincronizados en el servidor, por eso no se pierden aunque se cambie de cliente.

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?**

- No puedo decir qué protocolo es mejor, todo depende de lo que necesitemos, si por ejemplo queremos crear una aplicación que pueda gestionar o enviar mails de una manera precaria y no necesite el uso de carpetas o mantener información de los mails en el servidor, debería inclinarme a usar el protocolo POP ya que es sencillo y tiene una funcionalidad reducida que se adecúa a lo que necesito. En cambio, si necesito hacer una aplicación que requiera un manejo de mails más complejos me decantaría por usar el protocolo IMAP ya que su funcionalidad es más extensa que la de POP y mantiene sincronización con el servidor.
Considero que el protocolo IMAP debería de utilizar más recursos del servidor ya que debe gestionar toda la sincronización de los datos de los mails con el mismo.

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 el caso de destinatarios múltiples del mismo dominio o de diferentes dominios entre MUA-MSA se pueden enviar más de un correo durante una misma conexión. En el caso de destinatarios múltiples del mismo dominio entre MTA-MTA se pueden enviar más de un correo durante una misma conexión, esto reduce la sobrecarga al

no necesitar establecer múltiples conexiones TCP para destinatarios que pertenecen al mismo dominio.

En el caso de destinatarios múltiples de diferentes dominios entre MTA-MTA se puede enviar correos a todos los destinatarios de ese dominio usando una sola conexión, pero necesitará abrir nuevas conexiones TCP para los otros dominios.

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

- Es posible que el MSA escuche en un puerto TCP diferente a los convencionales, pero esto implica que los MUA del dominio y la infraestructura de red (como cortafuegos y NAT) deberán configurarse correctamente para permitir el tráfico en ese puerto no estándar. Además, podría generar problemas de interoperabilidad y soporte, ya que la mayoría de las aplicaciones y servicios están diseñados para operar en los puertos estándar de SMTP.

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

- Es posible configurar un MTA para que escuche en un puerto diferente al estándar (25) pero es altamente desaconsejado debido a las implicaciones en la interoperabilidad, entrega de correos y la compatibilidad con otros servidores. El puerto 25 es un estándar universal para la entrega de correos entre servidores, y cambiarlo puede romper la comunicación con otros MTAs, causando fallos en la entrega de correos a nivel global.

10. Ejercicio integrador HTTP, DNS y MAIL

- Suponga que registró bajo su propiedad el dominio **redes2024.com.ar** y dispone de 4 servidores:
 - Un servidor DNS instalado configurado como primario de la zona **redes2024.com.ar**. (hostname: ns1 - IP: 203.0.113.65).
 - Un servidor DNS instalado configurado como secundario de la zona **redes2024.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.redes2024.com.ar>.
- a. ¿Qué información debería informar al momento del registro para hacer visible a Internet el dominio registrado?
- Al servidor autoritativo de **.com.ar** se le debería informar:
 - El NS de los servidores autoritativos de mi dominio **redes2024.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.

- **Los registros que deberían configurarse en el servidor de nombres serían:**

- redes2024.com.ar. 86400 IN NS ns1.redes2024.com.ar.
- redes2024.com.ar. 86400 IN NS ns2.redes2024.com.ar.
- redes2024.com.ar. 86400 IN MX 5 mail.redes2024.com.ar.
- ns1.redes2024.com.ar. 86400 IN A 203.0.113.65
- ns2.redes2024.com.ar. 86400 IN A 203.0.113.66
- mail.redes2024.com.ar. 86400 IN A 203.0.113.111
- webmail.redes2024.com.ar. 86400 IN CNAME correo.redes2024.com.ar.
- redes2024.com.ar. 86400 IN SOA ns1.redes2024.com.ar. root.redes2024.com.ar. 2024093000 86400 2419200 86400

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

Justifique.

- No, no es necesario que el servidor DNS acepte consultas recursivas, y es más, es recomendable que no lo haga por estas razones:
 - **Funcionalidad**
 - La funcionalidad del servidor DNS autoritativo es responder con los registros DNS correspondientes al dominio del cuál es autoritativo cuando se le consulte directamente.
 - **Seguridad**
 - Habilitar la recursividad en un servidor autoritativo lo hace vulnerable a ciertos tipos de ataques como lo pueden ser los ataques de amplificación DNS. También puede exponerse a intentos de manipulación de caché o a ser usado como un recurso para resolver dominios maliciosos.
 - **Desempeño**
 - Aceptar consultas recursivas consume más recursos del servidor DNS, ya que implica que este debe resolver nombres de dominios externos, lo que aumenta la carga de trabajo innecesariamente para un servidor cuya principal función es responder a consultas sobre su propia zona.
 - **Separación de roles**
 - Normalmente, los servidores autoritativos están separados de los servidores recursivos. Esta separación de funciones mejora la seguridad y la eficiencia.

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

- **Protocolos que configurarías:**

- Para los servidores DNS configurarías el protocolo DNS sobre TCP o UDP, depende el tamaño de la consulta.
- Para el servidor de correo configurarías los protocolos SMTP e IMAP.
- Para el servidor web configurarías el protocolo HTTPS sobre TCP.

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

- **Puertos que considero que es necesario dejar abiertos:**

- Para los servidores DNS (ns1 y ns2) que usan como protocolo de transporte TCP dejaría abierto el puerto 53 para DNS.
- Para el servidor de correo que usa como protocolo de transporte TCP dejaría abiertos los puertos 25 para SMTP y 143 para IMAP.
- Para el servidor web que usa como protocolo de transporte TCP dejaría abierto el puerto 443 para HTTPS.

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

- El servidor webmail actúa como un MUA para los usuarios así que **en caso de tener que enviar un mail se conectaría de la siguiente forma con el servidor de correo:**

- El usuario accede al servidor webmail vía HTTPS desde su navegador y redacta el mail a enviar, luego, el servidor webmail se conectará con el MSA usando el protocolo SMTP para poder enviarle el mail que se desea enviar y este MSA se ocuparía de enviárselo al MTA emisor para que este lo envíe vía SMTP al MTA receptor en el servidor de correo. En caso de que el MSA esté integrado en el MTA emisor, el servidor webmail que actúa como MUA se conectará vía SMTP directamente con el MTA emisor.

En caso de recibir mails la conexión sería:

- El usuario accede al servidor webmail vía HTTPS desde su navegador para poder ver los mails del inbox, internamente, el servidor webmail usa el protocolo IMAP para recuperar los mails necesarios desde el servidor de correo.

g. **¿Cómo se podría hacer para que cualquier MTA reconozca como válidos los mails provenientes del dominio redes2024.com.ar solamente a los que llegan de la dirección 203.0.113.111? ¿Afectaría esto a los mails enviados desde el Webmail? Justifique.**

- El principal mecanismo utilizado para asegurarse de que cualquier MTA reconozca como válidos los correos electrónicos del dominio `redes2024.com.ar`. solo si llegan desde la IP `203.0.113.111` es **configurar los registros SPF (Sender Policy Framework)**
 - SPF es un mecanismo de autenticación de correos que permite a los servidores receptores (MTAs) verificar si un correo electrónico proviene de un servidor autorizado por el dominio que aparece en la cabecera "From". Para lograr esto, deberíamos configurar un registro SPF en nuestro servidor de nombres de la siguiente manera:
 - **`v=spf1 ip4:203.0.113.111 -all`**
 - **`v=spf1`** → indica que es un registro SPF de versión 1.
 - **`ip4:203.0.113.111`** → solo permite que los correos enviados desde esa IP sean considerados válidos.
 - **`-all`** → indica que cualquier otro servidor que intente enviar correos en nombre de `redes2024.com.ar`. debe ser rechazado.

El servidor webmail no debería verse afectado por esta nueva configuración siempre y cuando los correos enviados desde el webmail pasen por el servidor de correo que tiene la IP `203.0.113.111`

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)?

- Es necesario aplicar un encoding como por ejemplo base64 ya que estos protocolos fueron diseñados para soportar la transmisión de datos en formato de texto plano (ASCII) limitado a 7 bits. Imágenes, ejecutables y otros archivos binarios contienen bytes que no se ajustan a este formato, ya que utilizan una codificación de 8 bits o más. Para poder enviar estos archivos a través del correo electrónico, es necesario convertirlos a un formato de texto plano compatible con el protocolo.

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, es posible enviar un correo electrónico haciendo que el receptor vea un remitente distinto al real, y esto se conoce como "email spoofing". Esto se logra al manipular el header "From:" del correo electrónico, y es posible realizar esto debido a que SMTP no tiene un mecanismo intrínseco de autenticación del remitente. Esto significa que, al configurar un cliente o servidor de correo, un atacante puede modificar el campo "From" para que aparezca como si el correo proviene de cualquier dirección deseada. El "email spoofing" puede ser un indicador de una estafa o intento de phishing.

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 ve? ¿Es esto una indicación de una estafa? Justifique

- Sí, es técnicamente posible enviar un correo electrónico de manera que el receptor vea un destinatario (remitente) distinto al que realmente lo envió. Este proceso se conoce como email spoofing, y a menudo se utiliza en actividades maliciosas o engañosas. Esta manipulación se logra modificando la línea RCPT TO: del envoltorio del mensaje, la cual no es visible para el usuario final.

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?

- Nuestro MUA usará SMTP, se conectará con el MSA y va a necesitar los registros MX y AAAA mediante una consulta DNS.

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 se va a encargar de encolarlos hasta que se puedan enviar una vez se reinicie el servidor.

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?

- Necesitaría otro registro MX y otro registro A/AAAA para el servidor en la nube, además, habría que configurar prioridades en los registros MX dejando el local como el más prioritario y configurar al servidor en la nube para que acepte correos para nuestro dominio, de esta forma tenemos la tolerancia a fallos si es que el local no puede servir.

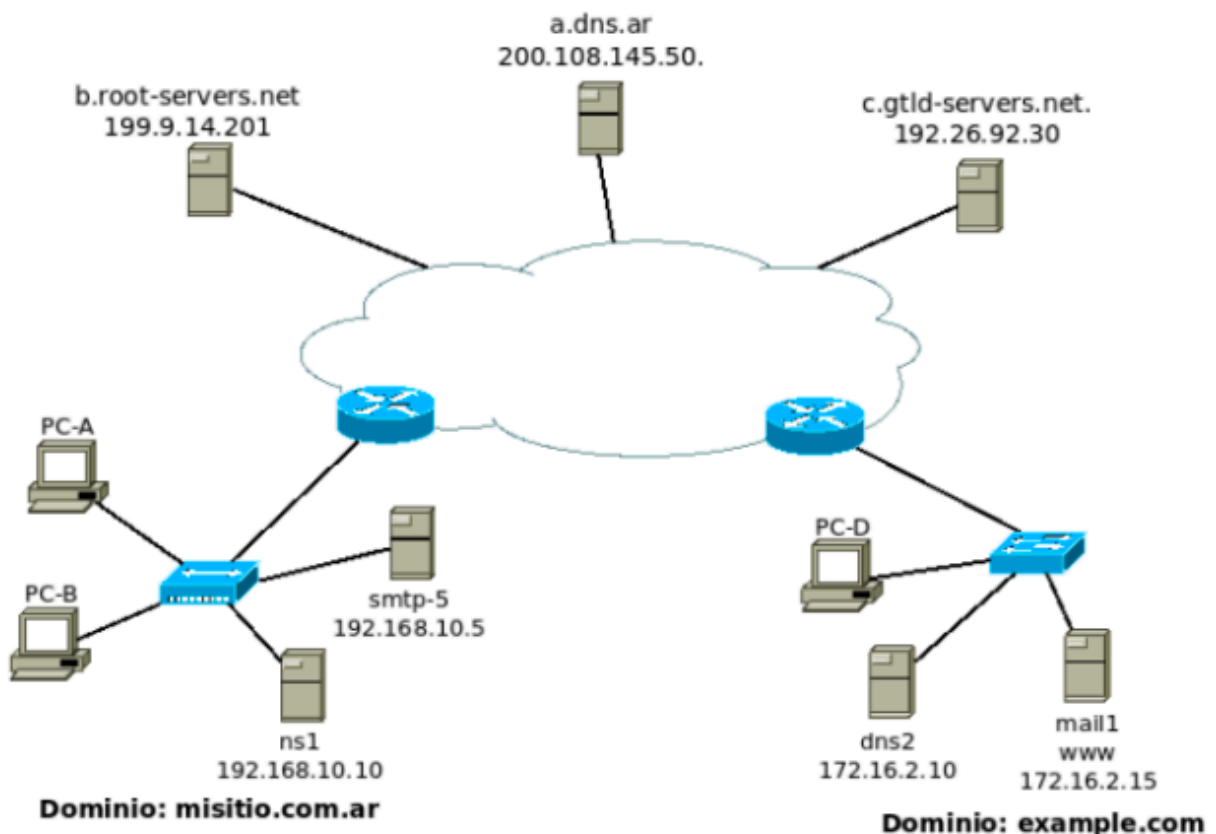
11. Utilizando la herramienta Swaks envíe un correo electrónico con las siguientes características:

- 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:

- 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.
 - ii. Indicar cuáles cabeceras fueron agregadas por la herramienta swaks.
 - iii. ¿Cuál es el message-id del correo enviado? ¿Quién asigna dicho valor?
 - iv. ¿Cuál es el software utilizado como servidor de correo electrónico?
 - v. Adjunte la salida del comando swaks y las fuentes del correo electrónico.
- b. Descargue de la plataforma la captura de tráfico smtp.pcap 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?
- 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 de `misitio.com.ar` no tiene la recursión habilitada
- a. El servidor de mail, mail1, y de HTTP, www, de `example.com` tienen la misma IP, ¿es posible esto? Si lo es, ¿cómo lo resolvería?
- Si, esto es posible, podríamos identificarlos únicamente por el número de puerto que estén escuchando.
- b. Al enviar el mail, ¿por cuál registro de DNS consultará el MUA?
- El MUA consultará por el registro A/AAAA del servidor SMTP que tenga configurado.
- c. Una vez que el mail fue recibido por el servidor smtp-5, ¿por qué registro de DNS consultará?
- Va a consultar por 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, es necesario realizar una consulta más, se consultará por el registro A/AAAA del servidor con mayor 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 ns1 tendrá que primero consultar por el **root server** más cercano que tenga para que le de la IP de un **servidor autoritativo** de `.com`, una vez obtenida la IP le consultará al autoritativo para que le de la IP de un servidor autoritativo de `example.com` y por último, una vez obtenida la IP del servidor autoritativo para `example.com`, le consultará para que le brinde los **registros MX** de los servidores de correo asociados a `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.**
 - **Falso.** El MSA se tiene que encargar de analizar los datos de la cabecera para saber si hay algún dato faltante.

- **Al ser recibidos por el servidor smtp-5 los datos agregados por el protocolo SMTP serán analizados por cada una de las capas inferiores.**
 - **Falso.** En el modelo de capas que utilizamos cada capa es responsable de procesar y encapsular los datos antes de pasarlos a la capa inferior, por lo que no son analizados por las capas inferiores.
 - **Cada protocolo de la capa de aplicación agrega una cabecera con información propia de ese protocolo.**
 - **Verdadero.** En la capa de aplicación protocolos como HTTP, SMTP, o FTP, agregan su propia cabecera con información relevante para ese protocolo en particular. Estas cabeceras contienen detalles como la dirección de destino, tipo de contenido, y otras informaciones específicas del protocolo que ayudan a la correcta interpretación de los datos.
 - **Como son todos protocolos de la capa de aplicación, las cabeceras agregadas por el protocolo de DNS pueden ser analizadas y comprendidas por el protocolo SMTP o HTTP.**
 - **Falso.** Cada protocolo tiene su propia estructura de cabeceras y formato de datos, no necesariamente deberían de estar diseñados para funcionar entre ellos 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.**
 - **Falso.** El protocolo HTTP brinda la abstracción necesaria para que los clientes puedan acceder al servidor HTTP independientemente de su 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.**
- No, no podrá. ns1 no es un servidor DNS recursivo, por lo tanto, no podrá resolver consultas para dominios que no sean los que administra directamente. Un servidor DNS autoritativo solo puede responder consultas para los dominios para los que tiene registros.
- h. **Cuando Alicia quiera ver sus mails desde PC-D, ¿qué registro de DNS deberá consultarse?**

- Por ninguno ya que el acceso a mails se gestiona con protocolos como POP o IMAP.
- i. **Indicar todos los protocolos de mail involucrados, puerto y si usan TCP o UDP, en el envío y recepción de dicho mail.**
- Se utiliza el protocolo SMTP en el puerto 25 y POP3 (puerto 110) o IMAP (puerto 143). Todos utilizan TCP.