Practica 6 Correo electrónico

SMTP

- Se usa para transmitir mensajes entre servidores
- Utiliza mensajes en formato ASCII 7 bits
- Utiliza el puerto 25

Comando	Descripción
HELO	Identificación del cliente, generalmente con un nombre de dominio.
EHLO	Permite al servidor declarar su aceptación de comandos ESMTP (Extended Simple Mail Transfer Protocol).
MAIL FROM	Emisor del mensaje.
RCPT TO	Receptor(es) del mensaje.
TURN	Permite al cliente y al servidor invertir los roles y enviarse mensajes en sentido contrario sin tener que iniciar una nueva conexión.
ATRN	Authenticated TURN. Tiene como parámetros opcionales uno o más dominios. Debe ser rechazado si la sesión no ha sido autenticada.
SIZE	Proporciona un mecanismo por el que el servidor SMTP puede indicar el máximo tamaño de mensaje admitido. Un cliente no debe enviar mensajes de mayor tamaño que el indicado por el servidor.
ETRN	Es una extensión de SMTP. ETRN lo envía un servidor SMTP para solicitar a otro servidor el envío de los mensajes que tenga.
PIPELINING	Permite enviar una sucesión de comandos encadenados sin esperas de respuesta a cada comando.
DATA	Lo envía el cliente para indicar que inicia el envío del contenido del mensaje.
DSN	Comando ESMTP que habilita el envío de notificaciones de estado del envío (Delivery Status Notification).
RSET	Anula la transacción completa y reinicializa el buffer.
VRFY	Verifica que un buzón existe. Por ejemplo, 'VRFY Ted' verifica que el buzón 'Ted' existe en el servidor.
HELP	Devuelve una lista de comandos admitidos por el servidor SMTP.
QUIT	Finaliza la sesión.

- Ejemplo de mensaje

```
HELO pepito.es
>250 servidor.es
MAIL FROM: pepe@pepito.es
>250 2.1.5. OK
RCPT TO: usuario@servidor.es
>250 2.1.5. Ok
DATA
>354 Start mail input; endi with <CRLF>.<CRLF>
subject: Asunto
Este mensaje es de prueba.
Probamos el protocolo SMTP.

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

- Tanto este protocolo como el resto son protocolos SIN seguridad
  - Por esto mismo, algunos servidores comerciales le añaden una capa de seguridad (hotmail, gmail, ...)
  - Esto se puede hacer de varia maneras
    - Una opción es: Una vez iniciada la conexión, activar al encríptación por TLS. Para ello:
      - el servidor admite el comando STARTTLS
    - Hacer esto manualmente es muy complicado por lo que haremos uso de openssl que se encargará de la encriptación

      ```
      openssl s client -starttls smtp -crlf -connect servidor.com:25
      ```

    - La segunda opción:
      - Iniciar una sesion de SMTP ya encriptada con SSL desde el principio
      - Consiste en empezar una conexion por el puerto 465

```
openssl s client -crlf -connect servidor.com:465
```

- Para cualquiera de las 2 opciones, es necesario autentificarse con el comando LOGIN
  - Esta info se enviará al servidor recodificada en base64 (representa un flujo de bits en bloques de 6 bits)

```
openssl s_client -crlf -connect servidor.com:465
>CONNECTED(00000000003)

...establecimiento de la conexión ssl...

>220 mx.google.com ESMTP i8sm55243855eeo.16
ehlo usuario
>250-mx.servidor.com at your service, [193.146.8.29]
>250-SIZE 35882577
>250-8BITMIME
>250-AUTH LOGIN PLAIN XOAUTH XOAUTH2
>250 ENHANCEDSTATUSCODES
auth login
>334 VXNlcm5hbWU6
usuario recodificado a base64
>334 UGFzc3dvcmQ6
contraseña recodificada a base64
>235 2.7.0 Accepted
mail from:<usuario@servidor.com>
>250 2.1.0 OK i8sm55243855eeo.16
rcpt to:<destino@otroservidor.com>
>250 2.1.5 OK i8sm55243855eeo.16
data
>354  Go ahead i8sm55243855eeo.16
subject asunto
Cuerpo del mensaje
```

POP3

- Tiene 3 fases de funcionamiento
- 1º La autenticación
  - el cliente envía los comandos `USER` y `PASS`
- 2º La transación
  - El cliente recupera los mensajes
  - Opcionalmente, puede marcar los mensajes que quiere borrar
- 3º La actualización
  - Cuando el cliente termina la sesión

- La comunicación se realiza por comandos ASCII

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

- Ejemplo de conexión

  -openssl s_client -crlf -connect servidor.com:465

  -user usuario

  -pass contraseña

  -list

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

IMAP

- Permite a un cliente de correo gestionar los mensajes de un usuario en un servidor
- Con este protocolo NO es necesario descargar los mensajes del servidor

- Todos los comandos deben empezar por una etiqueta arbitraria ya que puede realizar varias tareas al mismo tiempo

Comando	Parámetros	Descripción
LOGIN	usuario contraseña	Entrada al sistema
LIST	referencia nombre de buzón	Muestra el listado de carpetas de correo del usuario
SELECT	nombre de buzón	selecciona un buzón para poder acceder a sus mensajes
EXAMINE	nombre de buzón	Igual que Select, pero no realiza modificaciones
FETCH	número de secuencia elemento(s) del mensaje	Obtiene elementos de un mensaje identificado por su número de secuencia.
SEARCH	criterio de búsqueda	muestra los mensajes que cumplen el criterio de búsqueda
STORE	número de secuencia característica valor de la característica	permite asignar el valor especificado a la característica especificada del mensaje identificado por su número de secuencia.
COPY	número de secuencia buzón	copia (sin borrar) el mensaje identificado por su número de secuencia al buzón indicado
EXPUNGE		borra los mensajes con la característica "\Deleted"

- Los mensajes tienen 2 identificadores
  - número de secuencia (el orden en el buzón)
  - UID (un identificador global único).
- Ejemplo

```
1 login "usuario"
"contraseña" >1 OK LOGIN
completed. 1 list "" "*"

>* LIST (\Marked) (\HasNoChildren) "/"  INBOX
     ...resto de listado de buzones... >1 OK LIST
```

```
completed. 1 select INBOX >*1 EXISTS >*1 RECENT
>*FLAGS (\Seen \Answered \Flagged \Deleted \Draft;
     ...resto de listado del buzón... >1
OK [READ-WRITE] SELECT completed. 1
fetch 1 body >* 1 FETCH (BODY[])
}3094}
     ...cuerpo del mensaje... >1 OK
FETCH completed. 1 store 1
+flags.silent (\Deleted) >1 OK STORE
completed. 1 expunge >* 1 EXPUNGE
>* 0 EXISTS
>1 OK EXPUNGE completed.
1 logout
>* BYE  Mensaje despedida.
>1 OK LOGOUT completed.
```

- SMTP

  Ejemplo

  -openssl s_client -crlf -connect servidor.com:465

  -ehlo usuario

  -auth login

  -Usuario_recodificado_base64

- POP3

  openssl s_client -crlf -connect pop.gmail.com:995

  user usuario

  pass contraseña

  list

  list 1

  retr 1 //descarga el mensaje

- IMAP

  openssl s_client -crlf -connect imap.gmail.com:993

  a login arquitarde1 contraseña

  a list "" "*" //listado general

  a select INBOX

  a fetch 1 body //obtener el cuerpo del

- quit mensaje 1
Contraseña_recodificado_base64 a logout

echo -n
"rudoodin@gmailVGVsUG80NS4=.com\TelPo45."
| openssl enc -
base64
AGFycXVpdGFyZGUxQGdtYVlsLmNvbQBAETIzNDU2Iwo=

openssl s_client
-crlf -connect
smtp.gmail.com:465

ehlo usuario

-auth login

-
Usuario_recodificado_base64

-
Contraseña_recodificado_base64

mail
from:arquitarde1@gmail.com
//emisor del
mensaje

rcpt
to:jmruiz@gmail.com
//receptor del
mensaje

data

Subject:
"prueba”

.

quit