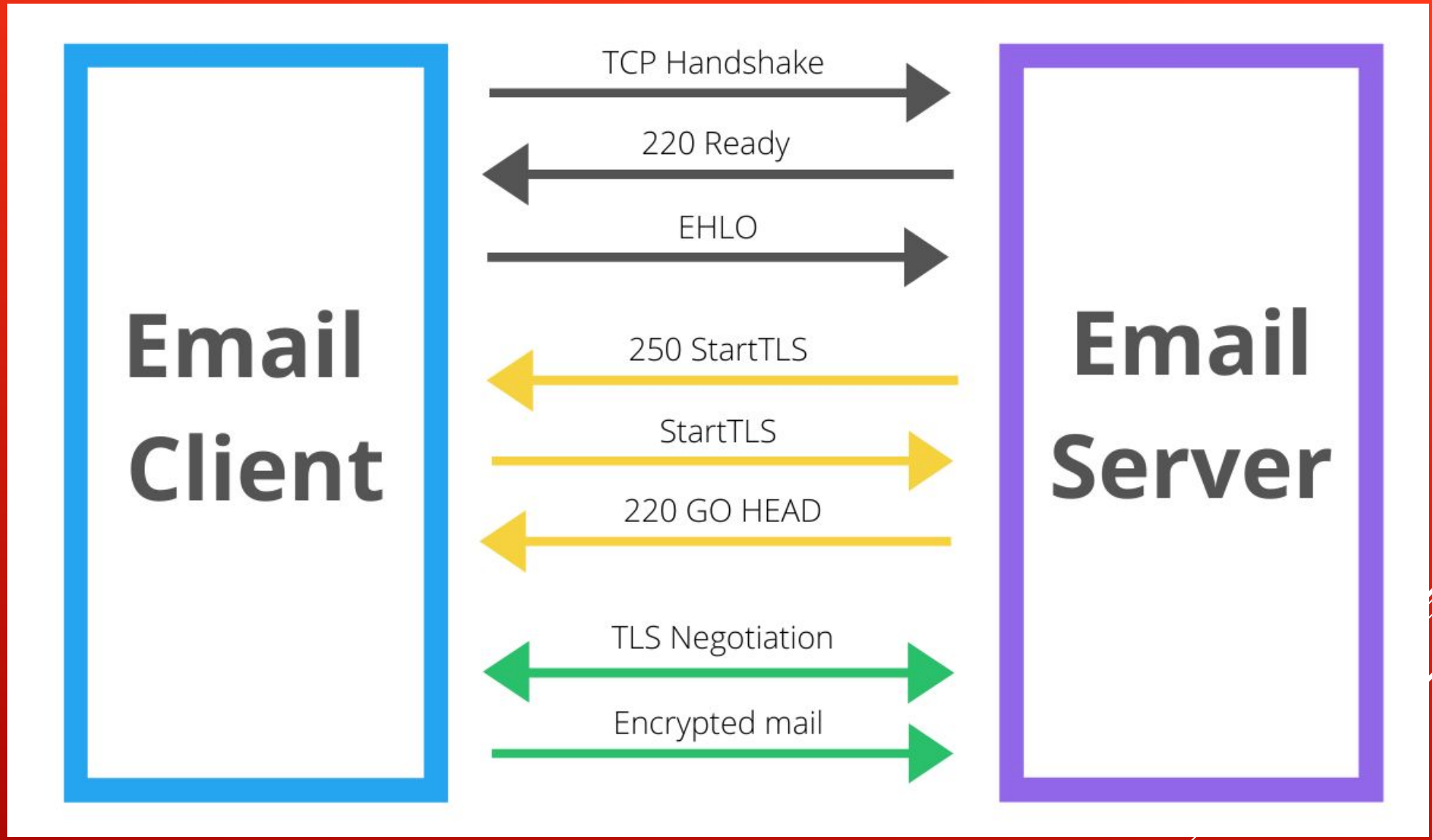
THE BRIDGE DIGITAL TALENT ACCELERATOR

SMTP

Simple Mail Transfer Protocol

@alejandromora
@amandaguglieri

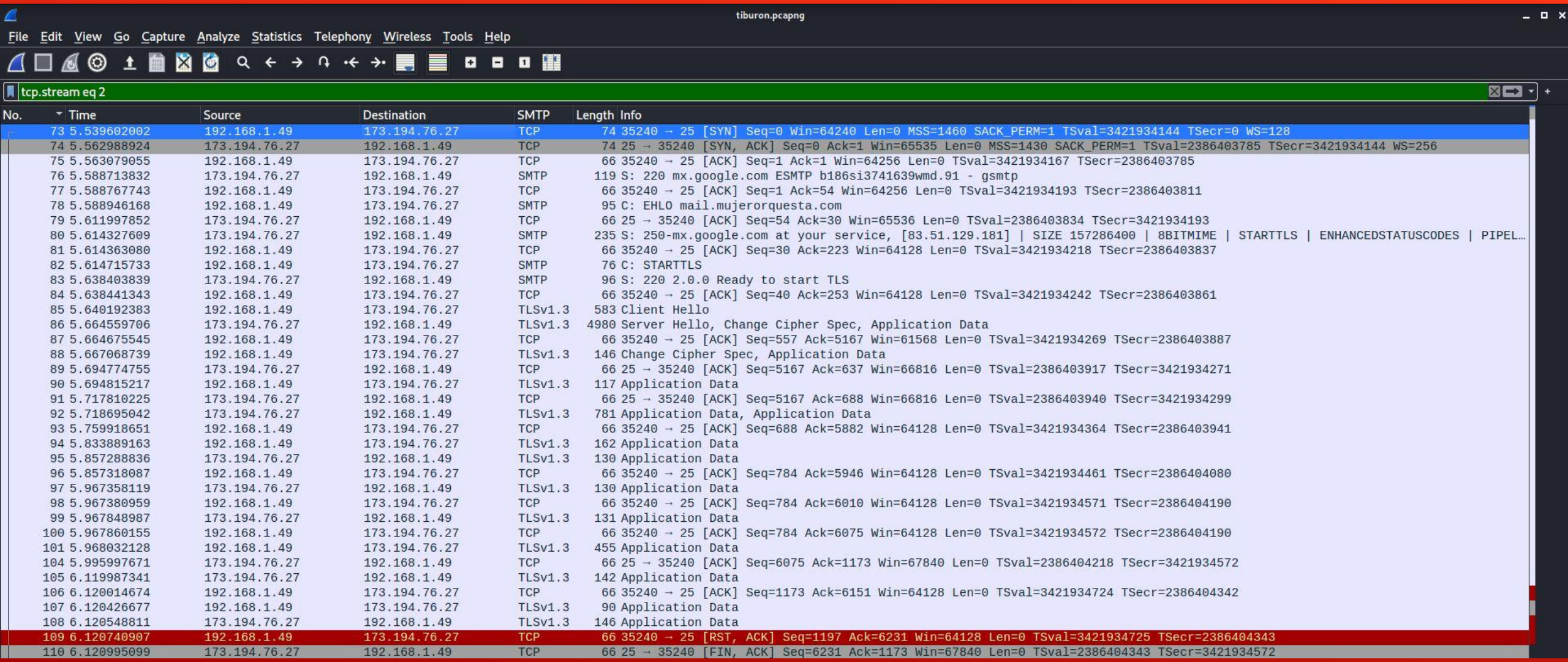
Capa TCP/IP	Capa de aplicación (SMTP), transporte (TCP) y red (IP).
Puertos	Los administradores de servidor pueden elegir si los clientes utilizan TCP puerto 25 (SMTP) o el puerto 587. El puerto 587 es el puerto por defecto para la presentación de SMTP en la web moderna. Aunque puedes usar otros puertos para el envío (más en los siguientes), siempre debes comenzar con el puerto 587 como el predeterminado y solo usar un puerto diferente si las circunstancias lo dictan (como si su host bloqueara el puerto 587 por alguna razón). El puerto 587 también soporta TLS, lo que significa que puedes enviar correos de forma segura. Aunque algunos servidores soportan el puerto 465. El puerto 465 fue registrado originalmente para SMTPS (SMTP sobre SSL). Después de un breve período en esa función, el puerto 465 fue reasignado para un uso diferente y desaprobado. A pesar de ello, muchos proveedores de servicios de Internet y de alojamiento en la nube siguen apoyando el puerto 465 para la presentación de SMTP. El puerto 2525 no es un puerto SMTP oficial (como lo reconocen el IETF o la IANA). Sin embargo, todavía se utiliza popularmente como alternativa al puerto 587 para la presentación de SMTP y la mayoría de los proveedores de servicios de Internet y de alojamiento en la nube sí admiten el puerto 2525 para SMTP.
Servicio que ofrece	
Envió en su versión más simple de correos electrónicos y con su versión extended la posibilidad de adjuntar otro tipo de contenido. Existen más versiones que permiten la encriptación (TCL), la autenticación del receptor con la extensión AUTH, entre otras extensiones.	
¿Cómo funciona? Y ¿Software típico que lo utiliza?	
El funcionamiento de este protocolo se da en línea, de manera que opera en los servicios de correo electrónico. Sin embargo, este protocolo posee algunas limitaciones en cuanto a la recepción de mensajes en el servidor de destino (cola de mensajes recibidos). Como alternativa a esta limitación se asocia normalmente a este protocolo con otros, como el POP o IMAP, otorgando a SMTP la tarea específica de enviar correos y recibirlos empleando los otros protocolos antes mencionados (POP o IMAP). El software más utilizado en diferentes SO. es Para Windows: Mailbird, TouchMail, eM Client, Outlook, para Mac: Mozilla Thunderbird, Polymail, Apple Mail y para Linux: Evolution, Mailspring, Claws Mail. Nosotros hemos instalado un servidor postfix sobre Kali para monitorizar con Wireshark la comunicación entre cliente y servidor. Adjuntamos prueba del funcionamiento donde recogemos algunos de los principales comandos de la sintaxis de SMTP: Helo/Ehlo, rcpt…	



https://sendgrid.com/blog/what-is-starttls/

LA CHICHA

Y LA LIMONÁ



No.	Time	Source	Destination	SMTP	Length	Info
73	5.539602002	192.168.1.49	173.194.76.27	TCP	74	35240 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3421934144 TSecr=0 WS=128
74	5.562988924	173.194.76.27	192.168.1.49	TCP	74	25 → 35240 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 TSval=2386403785 TSecr=3421934144 WS=256
75	5.563079055	192.168.1.49	173.194.76.27	TCP	66	35240 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3421934167 TSecr=2386403785
76	5.588713832	173.194.76.27	192.168.1.49	SMTP	119	S: 220 mx.google.com ESMTP b186si3741639wmd.91 - gsmtp
77	5.588767743	192.168.1.49	173.194.76.27	TCP	66	35240 → 25 [ACK] Seq=1 Ack=54 Win=64256 Len=0 TSval=3421934193 TSecr=2386403811
78	5.588946168	192.168.1.49	173.194.76.27	SMTP	95	C: EHLO mail.mujerorquesta.com
79	5.611997852	173.194.76.27	192.168.1.49	TCP	66	25 → 35240 [ACK] Seq=54 Ack=30 Win=65536 Len=0 TSval=2386403834 TSecr=3421934193
80	5.614327609	173.194.76.27	192.168.1.49	SMTP	235	S: 250-mx.google.com at your service, [83.51.129.181] | SIZE 157286400 | 8BITMIME | STARTTLS | ENHANCEDSTATUSCODES | PIPEL…
81	5.614363080	192.168.1.49	173.194.76.27	TCP	66	35240 → 25 [ACK] Seq=30 Ack=223 Win=64128 Len=0 TSval=3421934218 TSecr=2386403837
82	5.614715733	192.168.1.49	173.194.76.27	SMTP	76	C: STARTTLS
83	5.638403839	173.194.76.27	192.168.1.49	SMTP	96	S: 220 2.0.0 Ready to start TLS
84	5.638441343	192.168.1.49	173.194.76.27	TCP	66	35240 → 25 [ACK] Seq=40 Ack=253 Win=64128 Len=0 TSval=3421934242 TSecr=2386403861
85	5.640192383	192.168.1.49	173.194.76.27	TLSv1.3	583	Client Hello
86	5.664559706	173.194.76.27	192.168.1.49	TLSv1.3	4980	Server Hello, Change Cipher Spec, Application Data
87	5.664675545	192.168.1.49	173.194.76.27	TCP	66	35240 → 25 [ACK] Seq=557 Ack=5167 Win=61568 Len=0 TSval=3421934269 TSecr=2386403887
88	5.667068739	192.168.1.49	173.194.76.27	TLSv1.3	146	Change Cipher Spec, Application Data
89	5.694774755	173.194.76.27	192.168.1.49	TCP	66	25 → 35240 [ACK] Seq=5167 Ack=637 Win=66816 Len=0 TSval=2386403917 TSecr=3421934271
90	5.694815217	192.168.1.49	173.194.76.27	TLSv1.3	117	Application Data
91	5.717810225	173.194.76.27	192.168.1.49	TCP	66	25 → 35240 [ACK] Seq=5167 Ack=688 Win=66816 Len=0 TSval=2386403940 TSecr=3421934299
92	5.718695042	173.194.76.27	192.168.1.49	TLSv1.3	781	Application Data, Application Data
93	5.759918651	192.168.1.49	173.194.76.27	TCP	66	35240 → 25 [ACK] Seq=688 Ack=5882 Win=64128 Len=0 TSval=3421934364 TSecr=2386403941
94	5.833889163	192.168.1.49	173.194.76.27	TLSv1.3	162	Application Data
95	5.857288836	173.194.76.27	192.168.1.49	TLSv1.3	130	Application Data
96	5.857318087	192.168.1.49	173.194.76.27	TCP	66	35240 → 25 [ACK] Seq=784 Ack=5946 Win=64128 Len=0 TSval=3421934461 TSecr=2386404080
97	5.967358119	173.194.76.27	192.168.1.49	TLSv1.3	130	Application Data
98	5.967380959	192.168.1.49	173.194.76.27	TCP	66	35240 → 25 [ACK] Seq=784 Ack=6010 Win=64128 Len=0 TSval=3421934571 TSecr=2386404190
99	5.967848987	173.194.76.27	192.168.1.49	TLSv1.3	131	Application Data
100	5.967860155	192.168.1.49	173.194.76.27	TCP	66	35240 → 25 [ACK] Seq=784 Ack=6075 Win=64128 Len=0 TSval=3421934572 TSecr=2386404190
101	5.968032128	192.168.1.49	173.194.76.27	TLSv1.3	455	Application Data
104	5.995997671	173.194.76.27	192.168.1.49	TCP	66	25 → 35240 [ACK] Seq=6075 Ack=1173 Win=67840 Len=0 TSval=2386404218 TSecr=3421934572
105	6.119987341	173.194.76.27	192.168.1.49	TLSv1.3	142	Application Data
106	6.120014674	192.168.1.49	173.194.76.27	TCP	66	35240 → 25 [ACK] Seq=1173 Ack=6151 Win=64128 Len=0 TSval=3421934724 TSecr=2386404342
107	6.120426677	192.168.1.49	173.194.76.27	TLSv1.3	90	Application Data
108	6.120548811	173.194.76.27	192.168.1.49	TLSv1.3	146	Application Data
109	6.120740907	192.168.1.49	173.194.76.27	TCP	66	35240 → 25 [RST, ACK] Seq=1197 Ack=6231 Win=64128 Len=0 TSval=3421934725 TSecr=2386404343
110	6.120995099	173.194.76.27	192.168.1.49	TCP	66	25 → 35240 [FIN, ACK] Seq=6231 Ack=1173 Win=67840 Len=0 TSval=2386404343 TSecr=3421934572

FUENTES DE LAS QUE HEMOS BEBIDO

- https://es.wikipedia.org/wiki/Protocolo_para_transferencia_simple_de_correo
- https://sendgrid.com/blog/what-is-starttls/
- https://likegeeks.com/es/servidor-de-correo-linux-postfix/
- https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-postfix-as-a-send-only-smtp-server-on-ubuntu-18-04-es