Sobre protocolos de correo seguros y estegoanálisis de

[EMPRESA FARMACÉUTICA]

Fecha de realización: 03/04/2024

Consultoría realizada por:

Juan Luis Ruano Muriedas

José Joaquín Rojas Romero

Antonio José Suárez García

Índice

Resumen ejecutivo

Tras un exhaustivo estudio de su problema, nos gustaría proponerle las distintas **soluciones** a las que hemos llegado para cada una de sus consultas.

Para la ***Consulta 1*** hemos desarrollado un detallado tutorial para configurar su cuenta de correo en ***Mozilla Thunderbird*** y **generar una clave PGP**, así como **revocar** la misma en caso de verse comprometida y cómo **cifrar y/o firmar** sus correos.

Para la ***Consulta 2*** le proponemos un método para la **clasificación de correos no deseados** que se ajuste a sus necesidades y además le explicamos por qué es necesario mantener su correo seguro de *beacons o bitácoras* que puedan poner en **peligro su empresa.**

Para la ***Consulta 3*** hemos **analizado las imágenes recibidas** como pruebas ante la posible inclusión de un mensaje a través de esteganografía y **se han encontrado anomalías** en 2 de las imágenes recibidas. La información recibida de las imágenes se ha enviado al correo proporcionado como se indicó para garantizar la confidencialidad ante la sensibilidad de la información que se ha filtrado.

Metodología y resultados

Consulta 1

Para el problema que nos presenta recomendamos el uso de ***Mozilla Thunderbird***, ya que su configuración para usar PGP en el envío y recepción de correos es el más sencillo y seguro.

1. Una vez instalado *Thunderbird*, introduzca su nombre, correo electrónico y contraseña maestra(Figura 1). **Tenga en cuenta que esta será la contraseña maestra que mantendrá a salvo sus claves privadas**, por lo que asegúrese de que es segura y robusta. En caso de que necesite ayuda creando una contraseña seguro no dude en consultarnos.

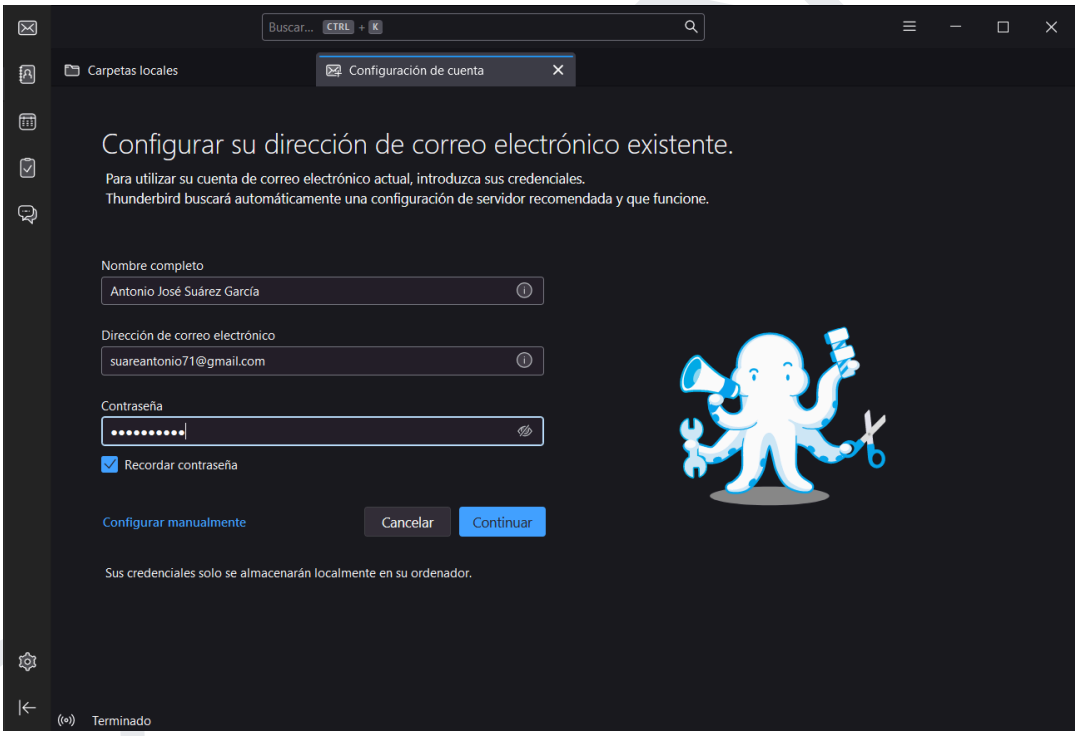

Figura 1. Primer paso de la configuración

2. Una vez introducidos los datos, haciendo clic en ***Configurar manualmente***, se abrirán más opciones para configurar los servidores de correos entrantes y salientes. Aclarar que si tiene un correo *Gmail* hay que hacer un paso extra antes de continuar. Deberá ir a *Gmail* y una vez ahí, haciendo click en el engranaje haga

click en Ver todos los ajustes. Una vez ahí vaya a ***Reenvío y correo POP/IMAP*** y seleccione la opción ***Habilitar IMAP***. Hecho esto podemos continuar en *Thunderbird*. En primer lugar, configuramos el servidor entrante con el protocolo IMAP, introducimos el nombre del servidor(al usar el protocolo IMAP el nombre de su servidor deberá ir precedido por *imap*, como se muestra en la Figura 2), introducimos el puerto 993(el puerto 993 es el **puerto seguro para IMAP** y funciona a través de cifrado TLS / SSL), seleccionamos SSL/TLS para la seguridad de la conexión, como método de autenticación seleccionamos OAuth2 y en nombre de usuario introducimos el correo electrónico que indicamos anteriormente. Para el servidor saliente la configuración es parecida. En primer lugar introducimos el nombre del servidor(el nombre del servidor saliente va precedido por smtp, tal y como se muestra en la Figura 2), el puerto 465(el objetivo del puerto 465 es establecer un puerto para que el protocolo SMTP opere con la capa de puertos seguros (SSL)**),** seleccionamos SSL/TLS para la seguridad de la conexión, como método de autenticación seleccionamos OAuth2 y en nombre de usuario introducimos el correo electrónico que indicamos anteriormente. Una vez hecho esto hacemos click en ***Volver a comprobar*** y, si todo es correcto, obtendremos un mensaje en verde que nos dice que todo está bien.

Finalizamos la configuración inicial haciendo click en ***Hecho***.

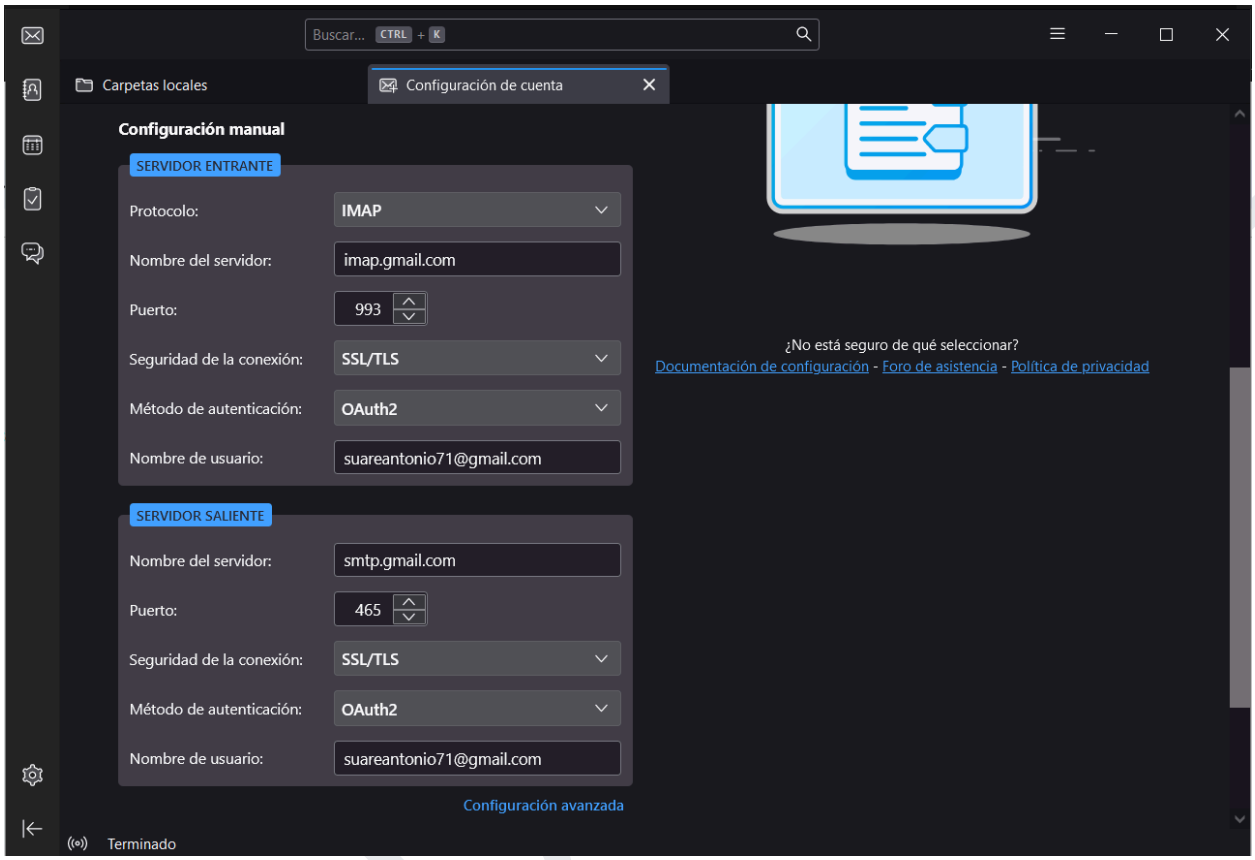

Figura 2. Configuración manual de los servidores en Thunderbird.

3. Una vez se haya iniciado nuestra cuenta en Thunderbird ya podremos enviar y recibir correos, pero aún no están protegidos por PGP. Para ello vamos a ***Configuración de la cuenta***(esquina superior derecha) y una vez ahí vamos a ***Cifrado extremo a extremo***. Aquí se mostrarán nuestras claves PGP. Haciendo click en Añadir clave pasaremos a la ventana para crearla. Seleccionamos ***Crear una clave OpenPGP*** y al continuar seleccionamos la fecha de caducidad de la misma(dada la importancia de los datos de su negocio, recomendamos un tiempo bajo, que no supere los seis meses) y en la *Configuración avanzada* seleccionamos el tipo de clave y su tamaño. Recomendamos el uso de RSA con 4096 bits, el cual le ofrecerá la mayor protección. Una vez hecho esto, hacemos click en ***Generar clave*** y esperamos a que se genere.

Ahora su clave PGP ya ha sido creada y desde ese mismo menú puede gestionarlas. Thunderbird las mantiene seguras, pero es posible que se vean comprometidas su computadora o su clave maestra. En estos casos es posible revocar las claves, informando

de que esas claves ya no son seguras. Para revocar una clave volvemos al menú anterior ***Cifrado extremo a extremo*** donde se listan nuestras claves. Una vez ahí, seleccionamos la clave que queremos revocar y, haciendo click en el desplegable ***Más***, seleccionamos la opción ***Revocar clave***. Siguiendo el proceso se nos indica que Thunderbird automáticamente compartirá el certificado de revocación de la anterior clave con cualquier persona con quien comparta su nueva clave pública, evitando así que se vuelva a usar la antigua clave.

Para firmar un correo electrónico y enviar su clave pública, lo único que tiene que hacer es, en la vista de redacción de un correo, únicamente tiene que seleccionar la opción ***Firmar digitalmente*** en el desplegable ***OpenPGP***. Además desde ese mismo menú puede cifrar los correos, aunque también puede hacerlo haciendo click en el botón ***Cifrar***.

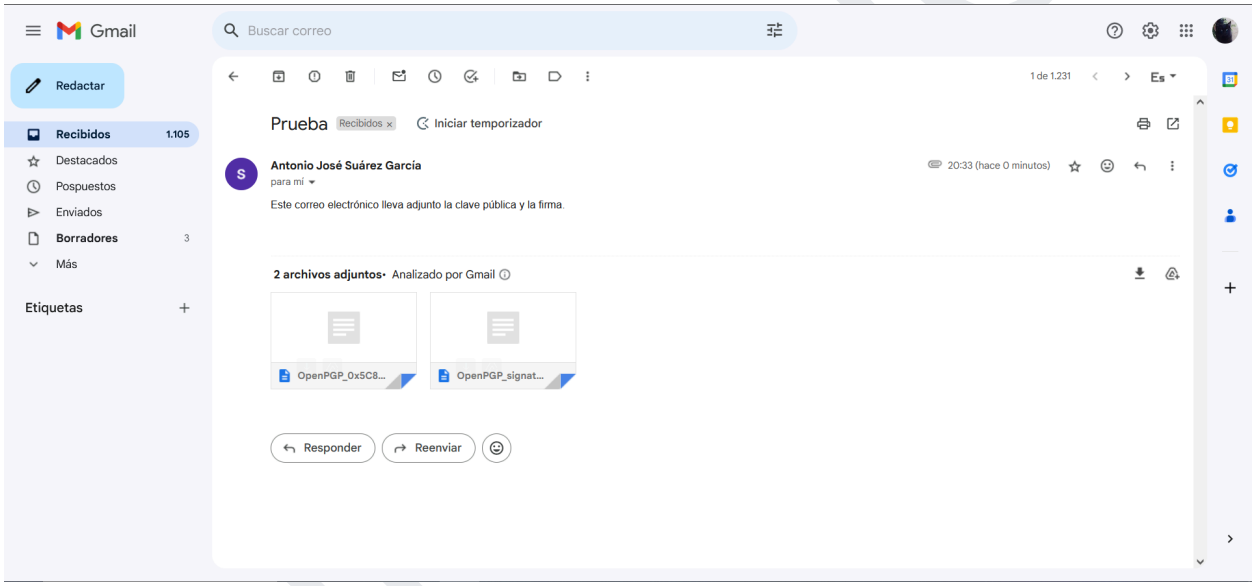

Figura 3. Correo recibido con la clave pública y la contraseña adjuntas.

Entendemos que todo este proceso puede ser un poco confuso, especialmente si no dispone de mucho conocimientos informáticos, así que no dude en contactar con nosotros para resolver cualquier duda al respecto.

Consulta 2

Para esta consultoría ustedes nos piden lo que se denomina un filtrado de correo no deseado para tácticas de **phishing** y **spear phishing**. El método que le recomendamos para ello es usando un algoritmo que haga uso de una **bolsa de palabras** como *naive bayes* o *tf-idf* y calcule la posibilidad de que un correo pueda llegar a ser malicioso basado en el el entrenamiento seguido y en el diccionario de palabras seleccionado con anterioridad el cual está basado en las características sobre correo no deseado.

El algoritmo en cuestión tendrá de entrada correos sin separar, con cabecera SMTP y payload y el primer paso deberá ser **normalizar los correos** o "limpiar" el correo, separando ruido de código HTML, signos de puntuación, preposiciones y reemplazando símbolos conocidos como el del dólar y normalizar los enlaces, los cuales empiezan por http y las direcciones de correo de manera que podamos mantener toda la **información relevante** lista para procesar separando cabecera y payload. Todo esto se podrá hacer, por ejemplo, en *Python* usando las librerías *nltk, bs4* y *EmailMessage* para la lectura y normalización de los correos.

A continuación se hará el diccionario con el cual entrenaremos el **algoritmo clasificador de correos** y es aquí donde pondremos en uso la información como por ejemplo las palabras más comunes de **publicidad**, palabras notorias en phishing como **amenazas**, **urgencias y llamadas de ayuda**, determinadas **marcas** del mercado, **datos propios** que pueden usar en nuestra contra, **información de las cabeceras** como Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting, and Conformance (DMARC), **Dirección IPs** de emisores conocidos, Dominio del emisor (Sender Domain), Detalles de enrutado (Detail routing), etc.

Todas las palabras elegidas compondrán lo que sería el vocabulario y a partir de aquí se debe entrenar con correos legítimos y no deseados, para ello usaremos la dataset de *Enron-Spam* que acumula gran cantidad de correos de pruebas precisamente para entrenar dichos algoritmos. Adicionalmente se podrían **añadir correos del usuario** a esta lista para ayudar aún más con el filtrado. El algoritmo aprende de ambas listas, una de no deseados y la legítima y creará uno o dos diccionarios (dependiendo del algoritmo) los cuales servirán para **validar los demás correos automáticamente** según la información recibida de este y el diccionario registrado previamente.

Tengamos por ejemplo que llega un correo **no deseado de phishing**, el algoritmo extrae el correo, lo normaliza y pasará a comparar el contenido con el diccionario registrado y decidirá que se trata de un contenido malicioso y por tanto debe ser eliminado. En el caso de ser un **correo legítimo**, pasará por los mismos pasos pero el algoritmo decidirá que no es necesario la eliminación del mismo.

La ventaja de este sistema es la gran capacidad de personalización del filtro por medio de la bolsa de palabras ya que podemos dotarlo con palabras que solo veamos en nuestro dia a dia de manera que podamos a hacer un **filtro más resistente al spear phishing.**

Es importante el análisis de correos electrónicos para la detección de posibles *beacons, bitácoras* o "etiquetas de seguimiento", las cuales se incrustan en correos electrónicos o páginas web y su propósito principal es **rastrear el comportamiento de los usuarios**, como sí han abierto un correo electrónico, cuánto tiempo han pasado viéndolo, qué enlaces han hecho clic, etc.

Cuando un usuario abre un correo electrónico que contiene un beacon, su cliente de correo electrónico descarga automáticamente la imagen (el *beacon*) desde el servidor del remitente. Esto informa al remitente que el correo electrónico ha sido abierto y proporciona detalles sobre el dispositivo y la ubicación del usuario en algunos casos.

Para **exfiltrar información empresarial**, un atacante podría incrustar un beacon en un correo electrónico que contiene información confidencial o sensible. Una vez que el destinatario abre el correo electrónico, el beacon se carga desde un servidor controlado por el atacante, lo que permite al atacante rastrear cuándo y desde dónde se ha abierto el correo electrónico. Esto **proporciona al atacante información valiosa** sobre los patrones de actividad del destinatario, como sus horas de trabajo, ubicación geográfica, dispositivo utilizado, entre otros detalles.

La mejor forma de evitar este riesgo es tener un **filtrado confiable y eliminar estos correos** mientras lo ignoran. Nuestro equipo tiene gran experiencia en filtrado de correos maliciosos y conocimientos sobre técnicas de fraude que pueden serle de utilidad en caso de que las necesite.

Consulta 3

El peritaje forense digital de las pruebas o evidencias aportadas por el cliente, ha determinado que la denuncia acerca del envío de información confidencial es **acertada**. Esto significa que, en efecto, **alguien está filtrando información confidencial fuera de la empresa farmacéutica**. En concreto, los ficheros: *Fichero3.png* y *Fichero4.png* han sido modificados mediante técnicas de esteganografía LSB (Less Significant Bit) con una reordenación de los canales RGB tal que BGR en el bit b1, siendo el ***Fichero4.png*** el más preocupante por contener la siguiente información reveladora en el mismo, la cual ha sido extraída mediante la herramienta **zsteg**.

A continuación, se mostrará más en detalle las capturas del proceso y los indicios que nos hicieron confirmar la denuncia.

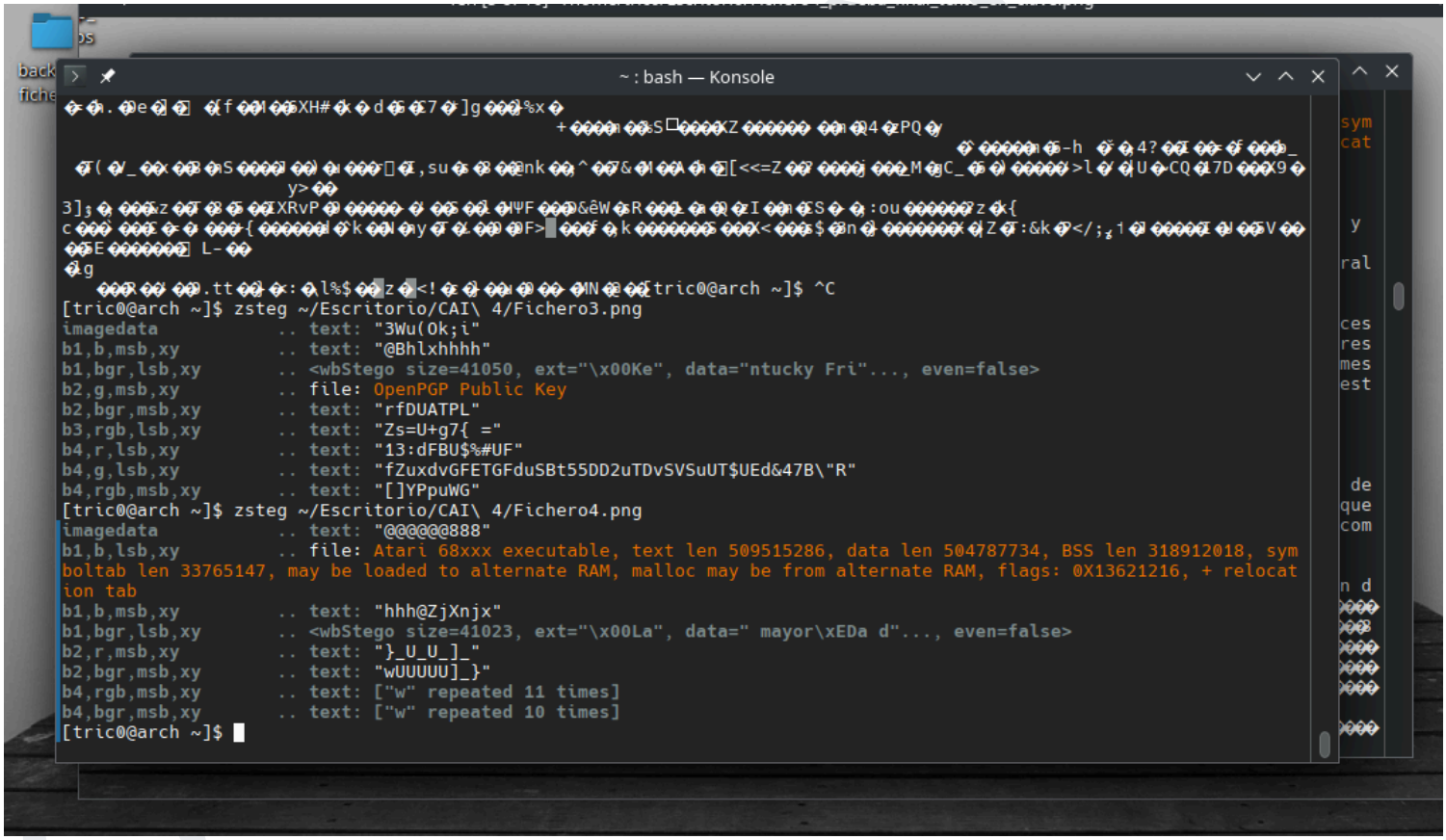

Figura 4. Uso de la herramienta zsteg a la ruta de los ficheros: *Fichero3.png* y *Fichero4.png*.

Los resultados muestran un contenido sospechoso en las líneas que comienzan por "<*wbStego*..." donde se deja entender, hilando los fragmentos de mensaje de los

parámetros “ext” y “data” de ambos archivos, un mensaje del estilo: “La mayor…Kentucky Fried Chicken”.

Decidimos analizar más en profundidad la posible modificación a través de técnicas LSB en el *Fichero3.png* del cual solo conseguimos extraer la línea tercera que se muestra en la **Figura 4**. Tras intentar decodificar cualquier posible texto en el ***Fichero4.png*** encontramos un texto que nos hizo evidenciar y verificar el motivo de su denuncia. En la **Figura 5** puede ver el resultado censurado de nuestra investigación.

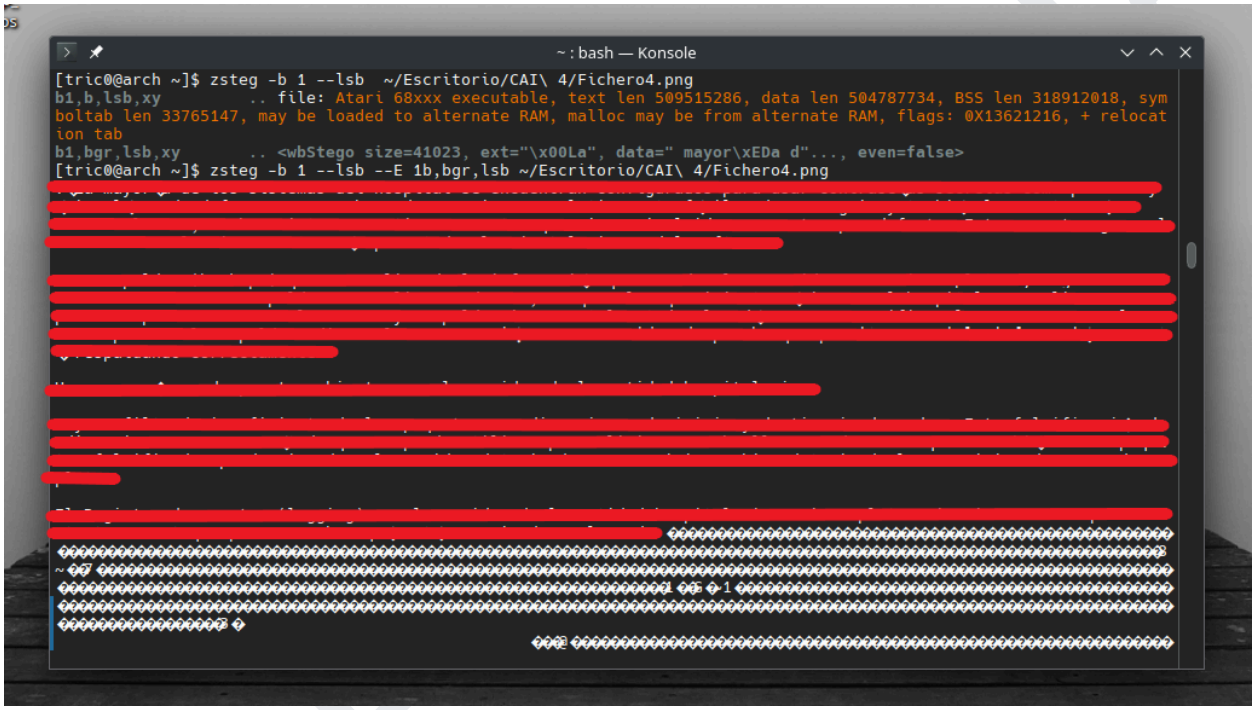

Figura 5. Uso de la herramienta zsteg con parámetros para indicar el bit, la técnica a emplear y los parámetros de extracción de información oculta en el *Fichero4.png*.

Las técnicas que se comentan han sido aplicadas a todos los ficheros de prueba adjuntos por el cliente, siendo los ficheros 3 y 4 los únicos que mostraron modificaciones o cambios en su integridad, resultando el *Fichero4.png* el que contenía la información filtrada.

Así mismo, las transformaciones realizadas por el responsable de filtrar la información han sido la alteración del orden de los colores RGB a BGR en el bit b1 con la técnica LSB.