Polo del Conocimiento

Pol. Con. (Edición núm. 98) Vol. 9, No 9
Septiembre 2024, pp. 1181-1194
ISSN: 2550 - 682X
DOI: 10.23857/pc.v9i9.7989

Análisis forense de seguridad mediante el uso de herramientas de escaneo en correos electrónicos de Gmail

Análisis forense de seguridad mediante el uso de herramientas de escaneo en correos electrónicos de Gmail

Análise forense de segurança mediante a utilização de ferramentas Gmail

Stiven Junior Ventura Díaz [I]
stiven.venturad@ug.edu.ec
https://orcid.org/0009-0009-3739-8378

Christian Omar Picón Farah [II]
christian.piconf@ug.edu.ec
https://orcid.org/0009-0003-8449-2064

Fausto Raúl Orozco Lara [III]
fausto.orozcol@ug.edu.ec
https://orcid.org/0000-0003-4872-3702

Correspondencia: stiven.venturad@ug.edu.ec

Ciencias Técnicas y Aplicadas
Artículo de Investigación

*** Recibido:** 26 de julio de 2024 ***Aceptado:** 24 de agosto de 2024 *** Publicado:** 12 de septiembre de 2024

I. Universidad de Guayaquil, Guayaquil, Ecuador.
II. Universidad de Guayaquil, Guayaquil, Ecuador.
III. Universidad de Guayaquil, Guayaquil, Ecuador.

Resumen

Este articulo surge como producto final del trabajo de titulación que tiene como tema Análisis forense de seguridad mediante el uso de herramientas de escaneo en correos electrónicos de Gmail de comerciantes del sector colibrí 1 en la parroquia Chongón, el objetivo de la investigación es mitigar vulnerabilidades expuestas por un análisis forense de seguridad aplicado a los correos electrónicos de comerciantes del sector de estudio. Para este caso, se ha empleado herramientas de escaneo especializadas y se aplicaron técnicas de análisis. Para su desarrollo, la metodología implementada abarca diversas fases, las cuales van desde la recopilación exhaustiva de datos, el análisis detallado de los metadatos, hasta la evaluación rigurosa de la autenticidad de los correos electrónicos para detectar posibles amenazas. Los resultados obtenidos permiten no solo identificar las principales vulnerabilidades existentes en la comunicación digital de estos comerciantes, sino también proponer medidas de seguridad concretas y efectivas para mitigar dichos riesgos.

Palabras Clave: análisis forense; mitigación; vulnerabilidades; correos electrónicos.

Abstract

Este articulo surgical como producto final del trabajo de titulación que tiene como tema Análisis forense de seguridad mediante el uso de herramientas de escaneo en correos electrónicos de Gmail de comerciantes del sector colibrí 1 en la parroquia Chongón, el objetivo de la investigación es mitigar vulnerabilidades expuestas Para este caso, se ha empleado herramientas de escaneo especializadas y se aplicaron técnicas de análisis. desde la recopilación exhaustiva de datos, el análisis detallado de los metadatos, hasta la evaluación rigurosa de la autenticidad de los correos electrónicos para detectar posibles amenazas. sino también proponer medidas de seguridad concretas y efectivas para mitigar dichos riesgos.

Keywords: análisis forense; mitigación; vulnerabilidades; correos electrónicos.

Resumo

Este artigo cirúrgico como produto final do trabalho de titulação que tem como tema Análise forense de segurança através do uso de ferramentas de varredura em correios eletrónicos do Gmail de comerciantes do setor colibrí 1 na paróquia Chongón, o objetivo da investigação é mitigar vulnerabilidades expostas Para este caso, foram empregues ferramentas de scan especializado e aplicadas técnicas de análise desde a recolha exaustiva de dados, a análise detalhada dos

metadados, até à avaliação rigorosa da autenticidade dos e-mails para detetar possíveis ameaças também. mitigar riscos.

Palavras-chave: análise forense; mitigação; de vulnerabilidades; de e-mails

Introducción

El presente proyecto aborda la problemática desde la aplicación de un análisis forense de seguridad a correos electrónicos de Gmail, al emplear este método, se busca identificar el tipo de vulnerabilidades a las que se enfrenta la población al llevar sus comunicaciones por este tipo de medios electrónicos. Siendo así, el problema es visto desde el punto de vista analítico con la recolección de la evidencia digital que sea necesaria, cumpliendo con cada fase de un análisis forense.

En un mundo digitalizado, el correo electrónico sigue siendo de las principales vías de comunicación tanto para usuarios individuales como para organizaciones, lo que lo convierte en un objetivo clave para diversas amenazas cibernéticas. Según un estudio de Verizon (2023), "el 94% del malware se entrega a través de correos electrónicos, lo que subraya la necesidad crítica de identificar y mitigar estas amenazas para proteger tanto la información personal como la corporativa". El comprender y atender dichas amenazas permite a las organizaciones y usuarios implementar medidas de seguridad más efectivas o reforzar las existentes, con el fin de reducir riesgos y mantener la integridad de sus datos.

El uso de tecnologías forense para la identificación de vulnerabilidades en medios electrónicos es sin duda alguna un tema que cada día toma más fuerza en un mundo digitalizado. A menudo se visualiza como gran parte de la población sufre ataques que tienes como fin irrumpir la privacidad y capturar sus datos para posteriormente cubrir un objetivo dependiendo la motivación del ciberdelincuente (Rochina Rochina, 2021).

El phishing es una forma de ciberdelincuencia que usa la ingeniería social como método para propagarse y el engaño tecnológico con el fin de capturar los datos requeridos que usualmente suelen ser usuarios y contraseñas de cuentas bancarias. Un ataque de ingeniería social surge de una motivación que regularmente es la parte económica, su funcionamiento se lleva a cabo mediante el uso de correos electrónicos falsos que pretenden ser de organizaciones comerciales de buena reputación, con el objetivo de capturar la información personal de la víctima, como direcciones de correo electrónico y contraseñas de sitios web no legítimos (Sustainability, 2023).

Para los comerciantes de la parroquia Chongón, lugar donde surge la problemática de esta investigación. Evidencia que, la creciente preocupación por la vulnerabilidad de sus datos a través de medios electrónicos como el correo, es una situación que no pasa desapercibida. Por esa razón, se apunta a la identificación del problema en base a el seguimiento de una serie de eventos que en los últimos meses han tenido como objetivo irrumpir la seguridad de los medios electrónicos de los habitantes del sector que es sujeto de este estudio. La tendencia muestra que gran parte de los atacantes buscan explotar vulnerabilidades mediante técnicas de ingeniería social, siendo el phishing uno de los ataques más comunes para explotar vulnerabilidades mediante los correos electrónicos.

El problema se ubica en el sector colibrí 1, en este sector posee un grupo de personas que se dedican al comercio, sus actividades van desde dueños de pequeñas tiendas, hasta vendedores de ropa y propietarios de bazares con varios locales distribuidos a lo largo y ancho de la parroquia. La importancia de elegir esta parte de la población como sujeto de estudio se justifica en base a la serie de inconvenientes que se atestiguó en los últimos meses en el sector y donde los comerciantes resaltaban como el objetivo principal de los ciberdelincuentes.

Adicionalmente, la evidente falta de conocimiento tecnológico asociada al cuidado de la información que se comparte por medios electrónicos figura para este caso como un problema que no puede pasar a segundo plano. De modo que, es una situación que no requiere de esfuerzos mayores para su corrección. Pero si puede ser la base de las soluciones que se vayan a exponer.

Metodología

Para este proyecto de investigación se eligió una metodología mixta, esta elección se fundamenta en la necesidad de abordar la complejidad del problema desde múltiples perspectivas y recopilar datos tanto cuantitativos como cualitativos, haciendo uso de instrumentos de investigación lo cual dependerá de la naturaleza de la información que se desea recopilar, todo esto con el objetivo de obtener una comprensión más sólida del tema de estudio.

Algunas de las características que se destacan con la elección de esta metodología son:

- **Complementariedad de enfoques:** Al combinar métodos cuantitativos y cualitativos, se aprovecha la complementariedad de ambos enfoques. Mientras que los métodos cuantitativos proporcionan datos numéricos objetivos sobre la frecuencia y la incidencia de ciertos aspectos como seria en este caso, el porcentaje de correos electrónicos con

características sospechosas, los métodos cualitativos permiten explorar en profundidad las percepciones, experiencias y contextos de los individuos involucrados, a lo que se podría destacar las percepciones de los usuarios sobre la seguridad de su correo electrónico.

- **Validación cruzada:** Los hallazgos cuantitativos pueden ser relacionados con evidencia cualitativa, y viceversa, lo que aumenta el nivel de credibilidad y fiabilidad de los resultados. Para este caso se podría tener en cuenta que, si los datos cuantitativos indican un alto porcentaje de correos electrónicos sospechosos, esta tendencia puede ser confirmada mediante el análisis obtenido a partir de las entrevistas cualitativas con los usuarios (Escudero Sánchez, C. L. & Cortez Suárez, L. A. , 2018).
- **Flexibilidad y adaptabilidad:** La utilización de una metodología mixta brindará una mayor flexibilidad y adaptabilidad generando un mejor ajustarse a las necesidades y características específicas del problema que se está investigando. Esto permite utilizar diferentes estrategias de recopilación y análisis de datos según sea necesario, lo que maximiza la eficacia y la relevancia de la investigación en el contexto particular de la seguridad de los comerciantes en el sector colibrí 1.

Enfoque cuantitativo

Para el desarrollo de la investigación se utilizaron técnicas cuantitativas con el fin de representar parte del problema y su respectiva solución mediante valores numéricos y asi generar una validación cruzada con los resultados cualitativos. De este modo, se pudo evidenciar los porcentajes de vulnerabilidad al aplicar herramientas de análisis de encabezados a los correos electrónicos.

Enfoque cualitativo

En este apartado se recurrió al uso de encuestas con preguntas abiertas para conocer el nivel de conocimiento tecnológico. Además, se realizó entrevistas a los participantes del análisis, logrando asi la obtención de resultados en base a la experiencia del sujeto de estudio.

Análisis forense de correos electrónicos

Se realiza el análisis forense utilizando las herramientas mencionadas previamente. Este análisis incluye la identificación de posibles amenazas, la detección de actividades sospechosas en los correos electrónicos y mitigación de vulnerabilidades.

A continuación, se presenta el proceso de análisis forense con el desarrollo de todas sus fases de manera secuencial.

Fase 1: Identificación

En esta fase se identificó que para este análisis forense lo recomendable sería trabajar con la copia de la mensajería del correo electrónico de los sujetos a investigarse. Siendo así, y con el respectivo permiso del propietario de la cuenta tal cual se adjunta el formato en los anexos, se procederá a generar un archivo de tipo MBOX, dicho proceso se detalla a continuación.

1. Se accede a la cuenta para proceder a generar la copia de los mensajes y archivos adjuntos de Gmail, donde se generará un archivo MBOX, como se evidencia en la figura 1.

Figura 1. Generación de documento MBOX con la copia de la mensajería

2. Una vez generada la copia, se procede con la descarga, como se muestra en la figura 2.

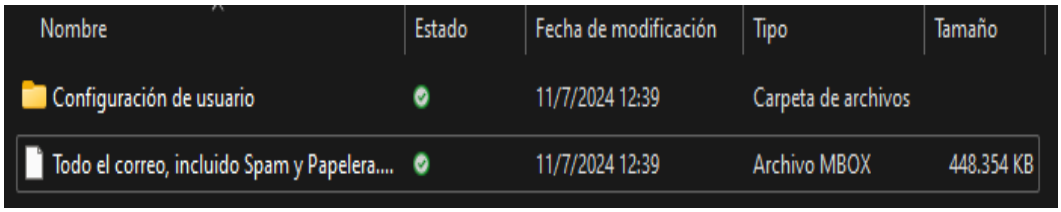

Figura 1. Descarga del archivo generado

Nota: Para medir el nivel de seguridad en los correos analizados se define como parámetro que los protocolos de seguridad deben dar como resultado un porcentaje superior al 80% para concluir que no existe una vulnerabilidad significativa dentro del proceso análisis de encabezados.

Fase 2: Preservación

En esta fase se busca mantener integra la información recopilada y por esa razón se almacena en carpetas con su respectiva copia de seguridad; donde el acceso sea gestionado únicamente por la

parte que lleva a cabo el proceso de análisis. El cumplir con estos pasos asegura la disponibilidad de la información, como se muestra en la figura 3.

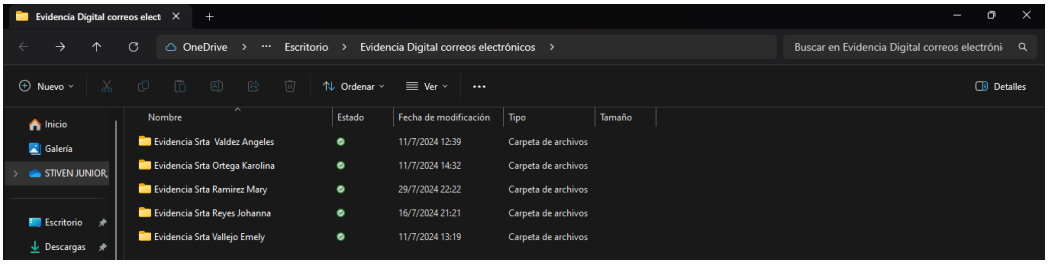

Figura 2. Guardado y cifrado de información

Fase 3: Extracción

En la fase de extracción se hace uso de herramientas especializadas para obtener resultados en base a un análisis forense de seguridad, a continuación, el detalle de las herramientas empleadas.

1. En primer lugar, se hará uso de la herramienta Aryson Mboxviewer, dicha herramienta ejecuta archivos Mbox y analiza la mensajería en varios formatos, de este modo se muestra el contenido de los mensajes de una forma más dinámica, como se visualiza en la figura 4.

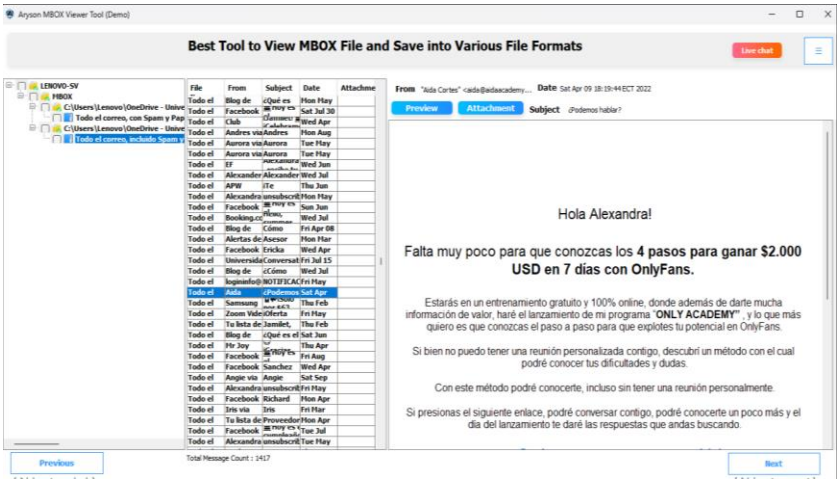

Figura 3. Extracción de información mediante la herramienta Aryson

2. Aquí se muestra la herramienta Systools MBOX Viewer, esta alternativa es similar a la anterior, de modo que al ingresar se debe seleccionar el tipo de aplicación, donde se va a seleccionar los archivos de tipo MBOX, como se muestra a continuación en la figura 5.

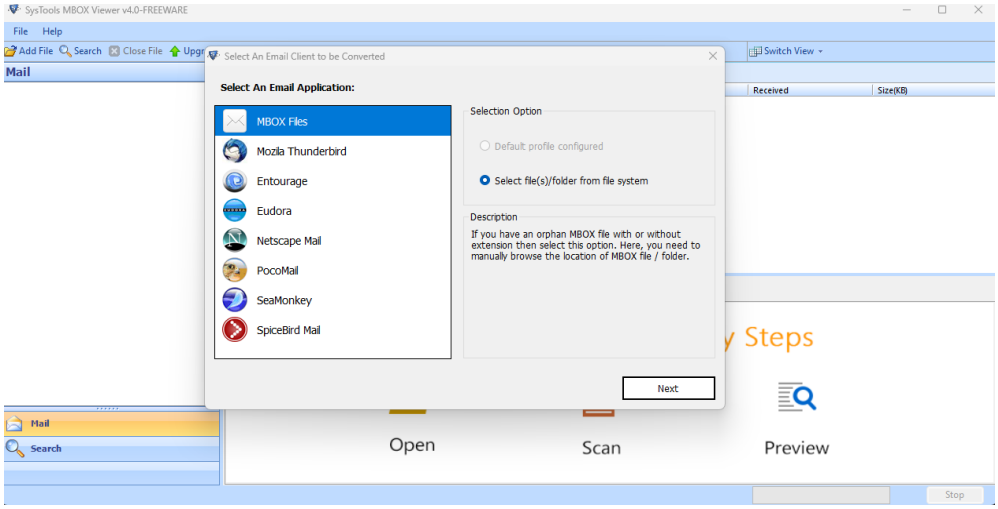

Figura 4. Extracción de información mediante la herramienta Systools

3. Una vez seleccionado el archivo que se ha generado de una copia de seguridad de la mensajería, se procederá a cargar el archivo en formato MBOX se cargan los mensajes y archivos que contenga la copia. Como se muestra en la figura 6.

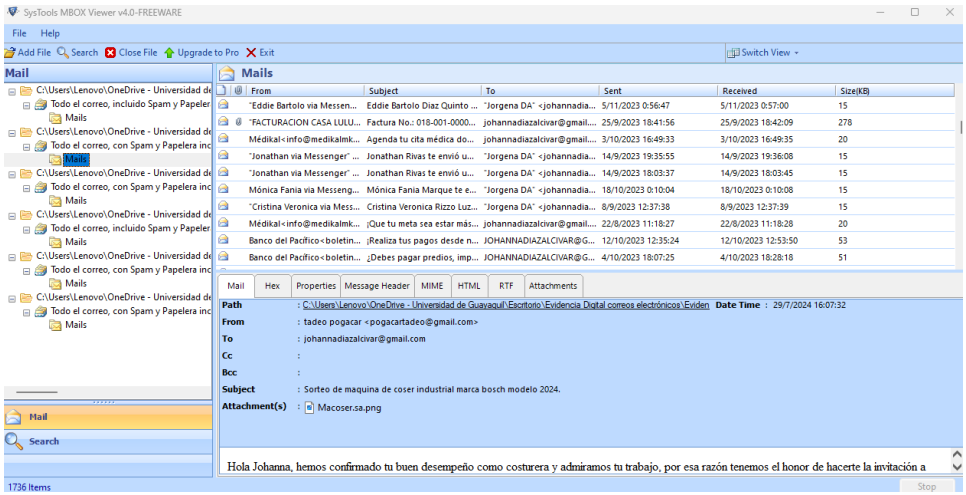

Figura 5. Información cargada al sistema

Fase 4: Análisis

En esta fase se procede al análisis de encabezados haciendo uso de las herramientas Email Header Analyzer y message Header. El objetivo de esta parte de los correos tiene como fundamento los resultados que se obtendrá en base a los protocolos de seguridad que intervienen al momento de analizar encabezados.

Para empezar con el análisis hay que tener en cuenta los siguientes protocolos que precisamente fueron diseñados como sistemas de protección:

1. **SPF:** Se utiliza para verificar el remitente. Es decir, el sistema reenviará un mensaje solo después de que se haya identificado la identidad del remitente. Esta comprobación se efectúa del lado de quien recibe el mensaje. Por esta razón, se destaca la importancia de configurar correctamente el protocolo (López Sánchez, 2019).

Los códigos que se usan para identificar el estado del mensaje son:

- **Pass.** La fuente es válida.
- **Fail.** La fuente no es válida.
- **Error.** Se produjo un error de comprobación.

2. **DKIM:** Realiza una comprobación criptográfica con el objetivo de verificar que el mensaje fue enviado por una parte autorizada.
3. **DMARC:** Cuando un mensaje no cumpla con las políticas de verificación para comprobar si un correo es el legítimo o no, este protocolo se encarga de definir como deberá actuar el servidor de correo receptor (DMARC, s. f.).

Luego de haber explicado el funcionamiento de los protocolos se exponen los resultados obtenidos en el análisis de cabeceras:

A continuación, se verifica que los protocolos SPF, DKIM y DMARC funcionan correctamente, se procede con selección de encabezados para su procesamiento mediante la herramienta Message Header, como se muestra en la figura 7.

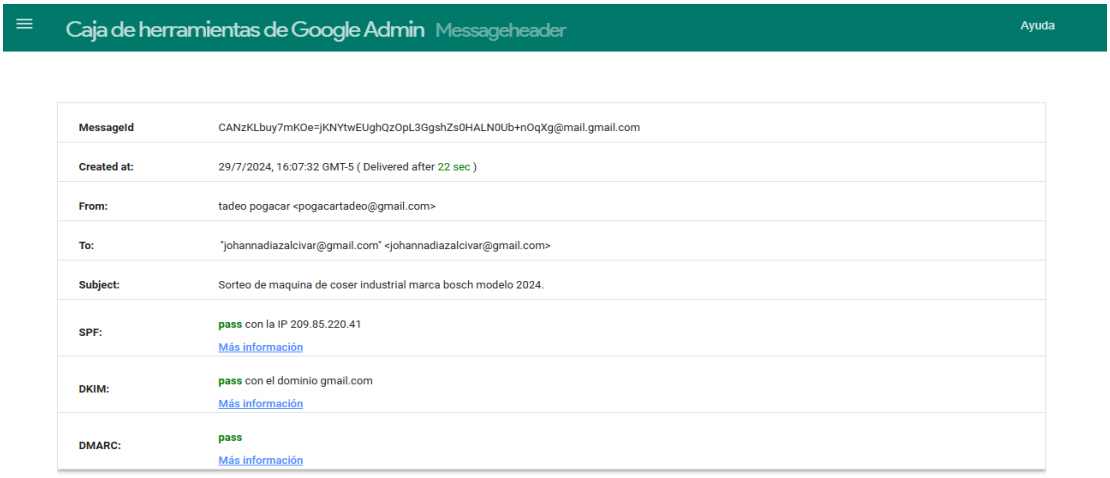

Figura 6. Protocolos de seguridad en el análisis de encabezados

Por otra parte, se realizará el mismo procedimiento del análisis de encabezados con la herramienta Email Header Analyzer. Esta herramienta a diferencia de la anterior ofrece un análisis más detallado de cada parte analizada del encabezado y el funcionamiento de cada protocolo se evidencia en cada paso con su respectivo indicador de cumplimiento o no, de las políticas de seguridad de seguridad, como se muestra en la figura 8.

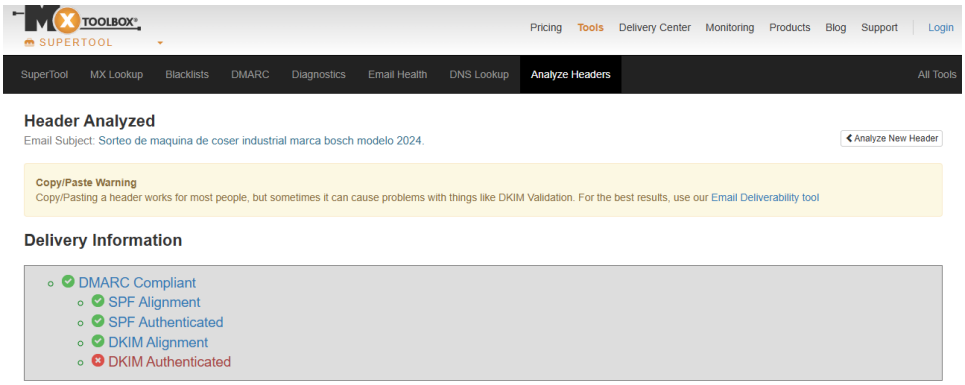

Figura 7. Resultados con la herramienta Email Analyzer Header

Con la correcta configuración de los protocolos SPF y DKIM aumenta el porcentaje de eficiencia del análisis y por ende los resultados indicarán con mayor precisión si existe alguna amenaza. De este modo, se puede identificar la autenticidad de cada correo analizado, como se evidencia en la figura 9.

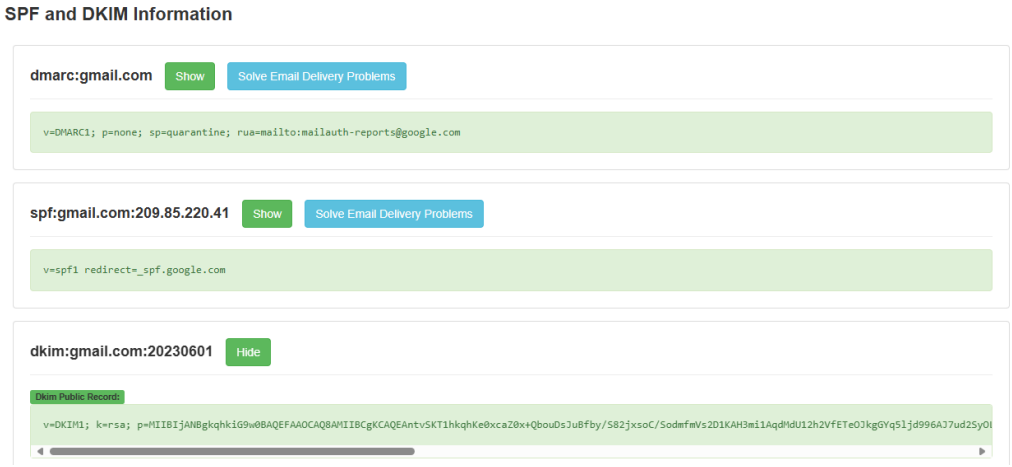

Figura 8. Análisis según protocolos de seguridad

Pol. Con. (Edición núm. 98) Vol. 9, No 9, Septiembre 2024, pp. 1181-1194, ISSN: 2550 - 682X

Fase 5: Documentación

En esta fase se entrega el informe con los resultados y las conclusiones obtenidas del análisis forense de seguridad a los correos electrónicos.

Resultados y discusión

Los resultados obtenidos del análisis forense se identificó una tendencia y esta se divide en dos partes, por un lado, los correos legítimos y por otro los intentos de suplantación.

- **Correo Legítimo:** La mayoría de los correos electrónicos analizados eran legítimos y procedían de fuentes autorizadas.
- **Intentos de Suplantación:** Se detectaron algunos intentos de suplantación de identidad en los correos electrónicos y aunque era evidente la señal de peligro, muchas personas desconocen cómo pueden facilitar sus datos en cuestión de segundos a ciberdelincuentes con el simple hecho de dar clic a un enlace.

Una vez concluido el proceso de análisis forense se procede a exponer los hallazgos encontrados al finalizar, como se visualiza en la tabla 1

Tabla 1. Resultados de análisis forense

Correo	Herramientas usadas	Amenazas detectadas	Evidencias encontradas
alexandravaldez895@gmail.com	Systools Mbox Viewer -Email analyzer Header	Ataques de phishing, mediante técnicas de ingeniería social(typosquatting)	Archivos maliciosos adjuntos a correos
johannareyes1116@gmail.com	Aryson Mbox Viewer- Message Header	Ninguna	Correos desconocidos a spam
eramos.ineval@gmail.com	Systools Mbox Viewer- Message Header	Ninguna	Correos desconocidos a spam

espinozajamileth24@gmail.com	Aryson Mbox Viewer-Email analyzer Header	Ninguna	Correos desconocidos a spam
lindaoyomaira25@gmail.com	Systools Mbox Viewer-Message Header	Spoffing	Enlaces e imágenes falsas
vergaralester400@gmail.com	Systools Mbox Viewer-Email analyzer Header	Ninguna	Ninguna
elena.ramirez.tamayo@gmail.com	Systools Mbox Viewer-Email analyzer Header	Ninguna	Ninguna
johannadiazalcivar@gmail.com	Systools Mbox Viewer-Email analyzer Header	Spoffing (typosquatting)	Enlaces de páginas web clonadas
luca.marvin1999@gmail.com	Aryson Mbox Viewer-Message Header	Ninguna	Correos desconocidos a spam
karolinaaylin.1993@gmail.com	Aryson Mbox Viewer-Message Header	Ataque de phishing	Archivos maliciosos
emelivallejo1999@gmail.com	Aryson Mbox Viewer-Message Header	Ninguna	Correos desconocidos a spam

La identificación y mitigación de vulnerabilidades parte de un correcto análisis de encabezados, esto a su vez va acompañado de la revisión de funcionamiento de protocolos de seguridad en correos electrónicos los cuales han sido mencionados previamente en parte de este trabajo. En la tabla 2 se muestra una breve descripción de cada uno acompañado de los resultados obtenidos.

Tabla 2. Análisis de encabezados de correos electrónicos

Protocolo	Descripción	Resultados
SPF (Sender Policy Framework)	Verifica si un correo fue enviado desde una fuente autorizada.	La mayoría de los correos electrónicos fueron enviados desde fuentes autorizadas.
DKIM (DomainKeys Identified Mail)	Permite verificar que un correo fue enviado y autorizado por el dueño del dominio del correo.	Los correos electrónicos analizados pasaron la verificación de DKIM, indicando que eran auténticos.
DMARC (Domain-based Message Authentication, Reporting, and Conformance)	Protege contra el uso no autorizado de un dominio de correo electrónico.	Algunos correos electrónicos no cumplieron con las políticas de DMARC, sugiriendo posibles intentos de suplantación de identidad.

Conclusiones:

- Se logró gestionar exitosamente el acceso a la información de los participantes del análisis, el establecer un buen nivel de confianza ayudó a que el proceso se lleve a cabo con un constante aporte mutuo.
- Se analizó los metadatos y toda la información que se pudo capturar de la evidencia recopilada, el escoger correctamente las herramientas de análisis hizo que esta fase se lleve a cabo sin ningún contratiempo.

Se identificó correctamente cuales serían las herramientas necesarias para el desarrollo de la parte práctica y consecuentemente se pudo evidenciar que los resultados obtenidos eran los previstos antes de empezar con el proyecto.

Referencias

DMARC. (s. f.). POWERDMARC. Obtenido de https://powerdmarc.com/es/what-is-dmarc/

Escudero Sánchez, C. L., & Cortez Suárez, L. A. . (2018). Técnicas y métodos cualitativos para la investigación científica. Obtenido de http://repositorio.utmachala.edu.ec/handle/48000/12501

López Sánchez, J. (2019). Métodos y técnicas de detección temprana de casos de phishing. Obtenido de http://hdl.handle.net/10609/89225

Rochina Rochina, C. (2021). Diseño y evaluación de una metodología para reducir los ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway. Obtenido de http://dspace.espoch.edu.ec/handle/123456789/14677

Sustainability. (2023). Email Security Issues, Tools, and Techniques Used in Investigation. Obtenido de https://doi.org/10.3390/su151310612

[6] Verizon. (2023). Data Breach Investigations Report 2023. Obtenido de https://www.verizon.com/business/resources/reports/dbir/?msockid=29a22d7782076ad624ad3f186076c0c