UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TÍTULO DEL TRABAJO DE TITULACIÓN

APLICACIÓN DE LA INFORMÁTICA FORENSE PARA IDENTIFICAR LA INTEGRIDAD DE UN CORREO ELECTRÓNICO

AUTOR

Quizhpilema Cruz Renzon José

Proyecto de Unidad de Integración Curricular

Previo a la obtención del grado académico en
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

Ing. Haz López Lídice Victoria

Santa Elena, Ecuador

Año 2023

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez Aquino, Mgt.
DIRECTOR DE LA CARRERA

Ing. Lídice Haz López, Mgt.
TUTOR

Ing. Daniel Quirumbay Yagual, Mgt.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel Suárez, Mgt.
DOCENTE GUÍA UIC

Ing. Mónica Jaramillo Infante, Mgt.
SECRETARIA

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por QUIZHPILEMA CRUZ RENZON JOSÉ, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 09 días del mes de agosto del año 2023

TUTOR

Firmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ

Ing. Lídice Haz López

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Quizhpilema Cruz Renzon José**

DECLARO QUE:

El trabajo de Titulación, Aplicación de la informática forense para identificar la integridad de un correo electrónico, previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 09 días del mes de agosto del año 2023

EL AUTOR

Renzon José Quizhpilema Cruz

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Quizhpilema Cruz Renzon José**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 09 días del mes de agosto del año 2023

EL AUTOR

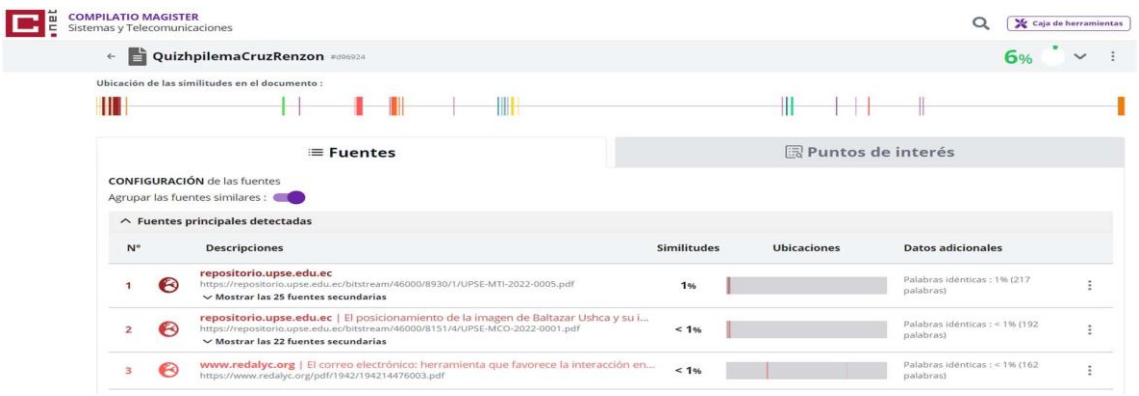
Renzon Quizhpilema Cruz

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado Aplicación de la informática forense para identificar la integridad de un correo electrónico, presentado por el estudiante, QUIZHPILEMA CRUZ RENZON JOSÉ fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 6%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



TUTOR

Firmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ

Ing. Lídice Haz López

VI

AGRADECIMIENTO

Agradezco a mis padres, por la confianza y darme todo el apoyo necesario para cumplir mis objetivos. Gracias por los valores y las enseñanzas que me brindaron.

A mi tutora, Ing. Lidice Haz Lopez por ser mi guía en este proceso de suma importancia, gracias por los conocimientos brindados y por haber aceptado ser mi tutora.

Renzon José Quizhpilema Cruz

DEDICATORIA

A mis padres, mi familia y en especial a mí, porque a pesar de las circunstancias pude lograr unos de mis objetivos en la vida.

Renzon José Quizhpilema Cruz

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo se estableció como finalidad aplicar métodos de computación forense para identificar la integridad de un correo electrónico enfocándose en el contexto de una institución de básica media, en donde el personal docente brindó información a través de una encuesta el uso del correo electrónico, gestión, herramientas de protección de datos personales y ciberataques relacionados con correos electrónicos conocidos. Para identificar huellas digitales relacionado con los ciberdelincuentes se utilizó herramientas de código abierto enfocado al análisis forense, además de utilizar la metodología UNE 71506:2013, la misma que se utiliza para el análisis de evidencia digital en la informática forense constando de 5 fases: Adquisición, Preservación, Análisis y Documentación. A través de todo lo expuesto con anterioridad mediante una evaluación manual se identifica el nivel de integridad de cada uno de los 6 casos asociados al proyecto actual.

Palabras claves: Ciberdelincuentes, correo electrónico, informática forense.

ABSTRACT

The present work was established to apply computer forensic methods to identify the integrity of an email focusing on the context of a middle school institution, where the teaching staff provided information through a survey on the use of email, management, personal data protection tools and cyber-attacks related to known emails. To identify digital fingerprints related to cyber criminals we used open source tools focused on forensic analysis, in addition to using the methodology UNE 71506:2013, the same that is used for the analysis of digital evidence in computer forensics consisting of 5 phases: Acquisition, Preservation, Analysis and Documentation. Through all of the above, by means of a manual evaluation, the level of integrity of each of the 6 cases associated with the current project is identified.

Keywords: 3 palabras

CAPITULO I. FUNDAMENTACIÓN

1.1. ANTECEDENTES

El envío de correos electrónicos es considerada como una actividad que permite intercambiar información de aspecto empresarial y personal; sin embargo, este método de comunicación también es mal usado por individuos que buscan aprovecharse de personas realizando estafas a través de correos electrónicos fraudulentos aplicando diversas técnicas de obtención de información como la ingeniería social u otros que involucran un uso avanzado de herramientas informáticas para cometer este tipo de delitos.[1].

Los fraudes relacionados con los correos electrónicos aumentaron su frecuencia con el surgimiento de la pandemia COVID-19 [2], tanto así que un gran porcentaje de personas conocen o han sido víctima de estos, y que además poseen un desconocimiento de este tipo de prácticas delictivas, las mismas que por desgracia no fueron advertidas o no fue posible identificar estos actos delictivos hacia ellos.

Según la revista Espacios el ataque informático más común es la infección a través de un malware siendo este mismo transmitido de diversos métodos desde medios físicos como la introducción de un hardware infectado hasta por medio de correos electrónicos en donde la víctima lo instala sin darse cuenta de aquello.[3]. (Ver anexo 1)

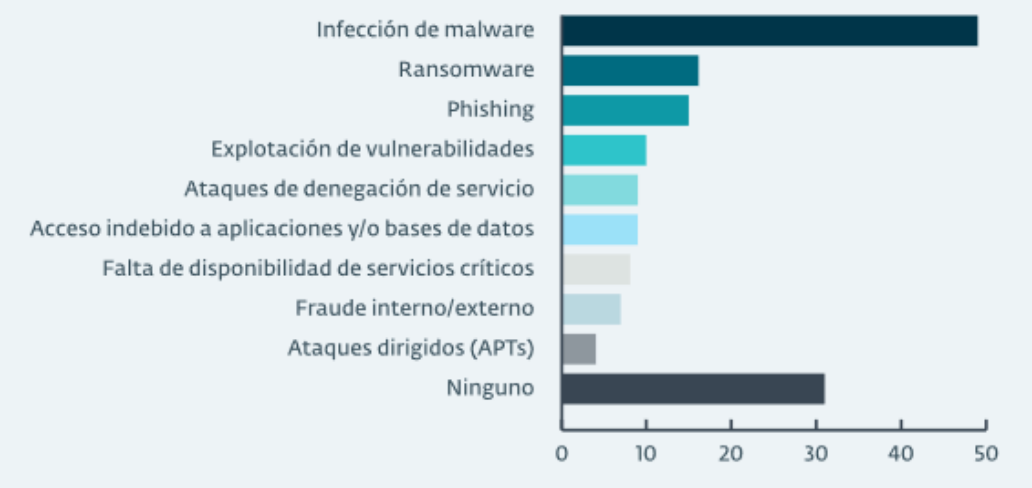


Fig. 1. Porcentaje de ataques informáticos a empresas y personas en Ecuador [4]

En el caso denominado United States of America v. Steve Waithe investiga un proceso judicial en el ámbito de acoso y fraude cibernético a través de redes sociales y correos electrónicos en donde se puede identificar que las fotos comprometedoras que involucraban a ciertas personas eran manipuladas además de adjuntar un mensaje con una premisa falsa.[5]

Según el autor de la anterior referencia existen varios métodos de fraudes electrónicos en general, pero este lo focaliza en 2 aspectos con relación a los correos electrónicos, los cuales son el acoso y fraude cibernético, el trabajo se centra en buscar huellas digitales y dar con el principal sospechoso de estos hechos que afectaron a adolescentes en su etapa estudiantil.

El trabajo mostrado por profesionales de la Institución Universitaria Tecnológico de Antioquia[6], presenta un análisis sobre los diferentes fraudes electrónicos y la mitigación que esta se da para cada uno de estos y haciendo un énfasis en los métodos para erradicar o no caer en este tipo de fraudes son los adecuados en las entidades financieras.

A través del análisis de la documentación referenciada se puede llegar a la conclusión de que las estafas mediante correos electrónicos pueden afectar incluso a empresas, tomando como ejemplo el caso anterior también a instituciones financieras considerando que todo el personal que forma parte de esta empresa debe tener conocimientos sobre cómo actuar frente a estos casos debido a la importancia de los datos electrónicos que esta maneja.

En otra investigación [7], se expone el proceso de análisis forense realizado a un servidor de correo electrónico en donde recalca algo muy importante que es el cálculo del riesgo para así tener una idea del impacto que puede tener una vulnerabilidad dentro de ese servidor.

El análisis de vulnerabilidades es muy importante que se realiza en las empresas o instituciones debido a que estas necesitan de alguna u otra manera poder mitigarlo si es posible para que no afecte de una manera relevante a la empresa o simplemente disminuir su impacto si esta vulnerabilidad se llega a explotar.

En consecuencia, en nivel de impacto o daño que puede causar este tipo de estafas mediante correos electrónicos va a depender mucho de la persona a la que va dirigido, es decir al perfil de la víctima ya que esta misma puede manejar información personal

importante (fotos, facturas, correos electrónicos, ubicaciones, movimientos bancarios, contactos, etc.) o para alguna institución o empresa (contratos, normas, órdenes de Compra, actividad financiera, etc.).

El análisis forense, según CSV, es considerado como el levantamiento de información e investigación de sucesos dañinos dentro de una organización o un ámbito en específico [8], el cual consisten en aplicar técnicas especializadas en obtener información de un hardware sin afectar o alterar su estado, lo que facilita buscar datos ocultos, dañados o eliminados.

En casos especiales se hace un análisis del perfil del atacante utilizando el modelo SKRAM, mismo nombre dado por sus siglas: Skill (habilidad), Knowledge (conocimiento), Resources (recursos), Access (acceso), Motive (motivo), este análisis consta de preguntas relacionadas directa o indirectamente con el ataque realizado a una institución [9].

Cuando existe la presencia de una brecha de seguridad se definen objetivos esenciales del uso de la informática forense [10]: ayudar a tener una idea del motivo y la posible identidad del atacante, diseño de procedimientos de una presunta escena de crimen, identificar el impacto potencial de la actividad maliciosa, preservar la evidencia siguiendo la cadena de custodia entre otras.

1.2. **DESCRIPCIÓN DEL PROYECTO**

Debido a la frecuencia de estos tipos de ataques informáticos relacionado con los correos electrónicos [3], se propone realizar un análisis informático forense para identificar los tipos de emails maliciosos y su manera de operar con el fin de elaborar un conjunto de buenas prácticas basado en un estándar internacional acerca de estos y las formas de no caer en estos engaños o ataques informáticos.

El peritaje informático es considerado como una técnica que ha crecido en los últimos años [11], este mismo se encuentra relacionada con casos de estudios en donde se dio alguna novedad relacionada con delitos financieros, evasión de impuestos, investigación sobre seguro, entre muchos más casos y campos a estudiar.

También, se realiza una encuesta utilizando un muestreo probabilístico a 51 docentes, de una institución de educación básica-media de la provincia de Santa Elena, con el fin de evaluar el nivel de conocimiento respecto al uso de la administración de las cuentas de correo electrónico y las ciberamenazas presentes a en este medio de comunicación.

El presente estudio se realiza utilizando la metodología de investigación correlacional con validación de hipótesis cuyo fin evaluar el nivel de correlación entre el número de ataques de correos electrónicos y la exposición de las personas a estas ciberamenazas; así como caracterizar las habilidades y conocimientos de los usuarios respecto al uso y la seguridad de los correos electrónicos.

Para realizar las pruebas experimentales se implementan 5 fases enmarcadas en la metodología UNE 71506:2013 para análisis de evidencias digitales, la misma que está vigente desde el año 2013 hasta la actualidad [12]:

- **Fase 1: Adquisición. –** Adquirir la evidencia digital a través de un repositorio en la nube para proceder al análisis.
- **Fase 2: Preservación. –** Verificar la autenticidad del email realizando una comparación de código hash de los correos electrónicos.
- **Fase 3: Análisis. -** Procesos y tareas que como finalidad intentarán dar una posible respuesta a preguntas que tienen relación con la investigación en curso.
- **Fase 4: Documentación. –** Se procede a documentar el procedimiento realizado a la evidencia digital, herramientas utilizadas, métodos y demás desde que inicia el análisis hasta la generación del informe pericial siguiendo una secuencia temporal definida.

La presente investigación requiere del uso de software que permiten realizar un análisis además de comprobar la autenticidad de los correos electrónicos adquiridos, a continuación, se procede a describir las herramientas mencionadas:

Sistema Operativo Caine: Distribución de Linux que ofrece un entorno forense adecuado el mismo que proporciona los diferentes softwares para realizar el correcto análisis de las evidencias digitales.[13]

QFileHasher: Software que permite calcular y verificar diferentes archivos con una GUI parecida, admite varios algoritmos de cifrados para códigos hash: MD4, MD5, SHA1, SHA2. [14]

ExtractMetadata: Software gratuito que permite extraer los metadatos de varios tipos de archivos tales como: Doc, Pdf, Mp3, Xls, Avi, entre otros. [15]

Ftk imager: Software recomendado para el análisis de la evidencia electrónica mediante la obtención de imágenes forenses [16].

VirusTotal: Herramienta web que realiza análisis de archivos, links, Url, Ip con el objetivo de encontrar anomalías en los datos proporcionados[17].

Message Header Analyzer Azure: Herramienta para visualizar encabezados de los mensajes de correo electrónico [18].

El presente proyecto contribuirá a la línea de investigación Tecnologías y Gestión de la Información, debido a que tiene relación con temas análisis forense usando herramientas de código abierto y la aplicación de métodos para evaluar la autenticación e integridad de varios correos electrónicos.

1.3. OBJETIVOS DEL PROYECTO

1.3.1. Objetivo General

- Realizar un análisis forense informático para identificar la integridad y confiabilidad de un mensaje de correo electrónico mediante la aplicación de procedimientos y herramientas de investigación criminológica.
- Determinar el nivel de exposición de ciberamenazas de los usuarios respecto al uso de los correos electrónicos mediante la aplicación de una encuesta.

1.3.2. Objetivos Específicos

- Realizar el proceso de adquisición de emails mediante herramientas forenses que garantice la preservación de la evidencia digital.
- Evaluar el nivel de conocimiento de los usuarios respecto al uso y gestión de los correos electrónicos como herramienta de comunicación mediante la aplicación de una encuesta.

- Realizar un análisis forense informático a los emails maliciosos con el fin de identificar su procedimiento y operatividad.
- Elaborar un informe técnico que describa los resultados del análisis forense efectuado a los emails de prueba.
- Elaborar un conjunto de buenas prácticas basado en normas internacionales ISO 27000 y NIST que describa procedimientos de seguridad informática para prevenir ser víctima de correos fraudulentos.

1.4. JUSTIFICACIÓN DEL PROYECTO

El uso del correo electrónico en diferentes ámbitos ya sea: laboral, personal o educativo, fomenta el fortalecimiento de la comunicación por lo que cabe destacar que su accesibilidad, interactividad, actualización constante y ahorra de tiempo y recursos lo vuelven una de las plataformas más útiles en las áreas antes mencionadas [19].

Según datos de la empresa de seguridad Kaspersky en el año 2021, el número de archivos maliciosos que fueron adjuntos en correos electrónicos aumentó de manera considerable en el tercer trimestre en comparación al segundo [20]. Es notable el número archivos dañinos adjuntos a este servicio de mensajería por lo que es necesario e importante tomar precauciones al hacer uso de este mismo para así evitar caer en este tipo de estafas.

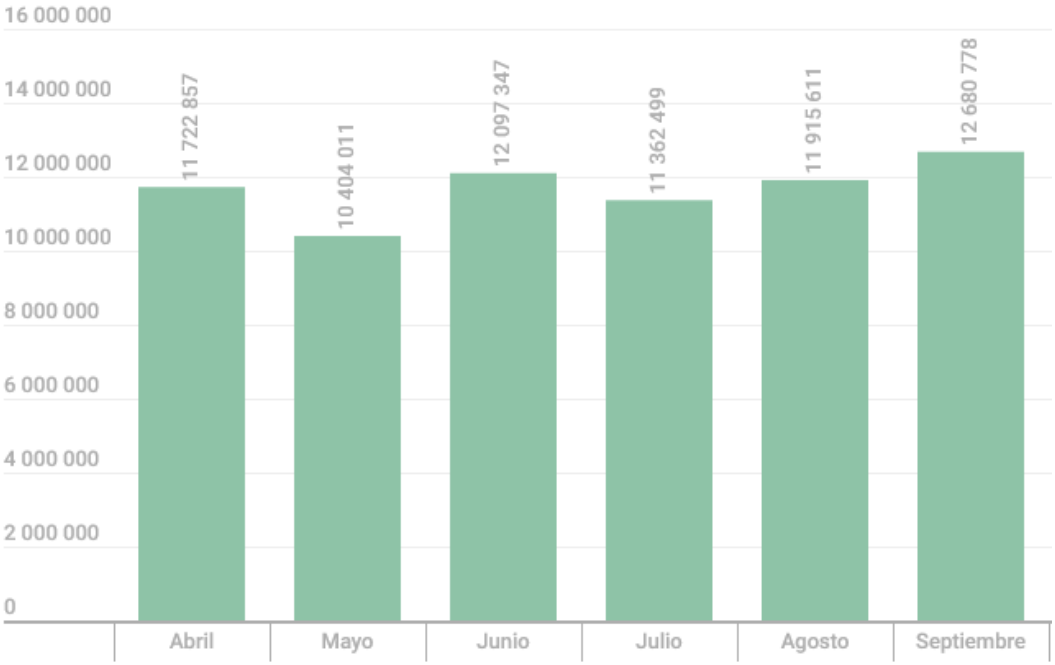


Fig. 2. Estadísticas de archivos maliciosos en correos electrónicos. [21]

Por otra parte, la misma fuente indica que en el tercer trimestre de 2021 los troyanos de la familia Agensla representada por el 9.74% se convirtieron en software malicioso más común en el spam de los correos electrónicos, así mismo, el autor de estas estadísticas indica los malware más comunes presentados en el correo electrónico.

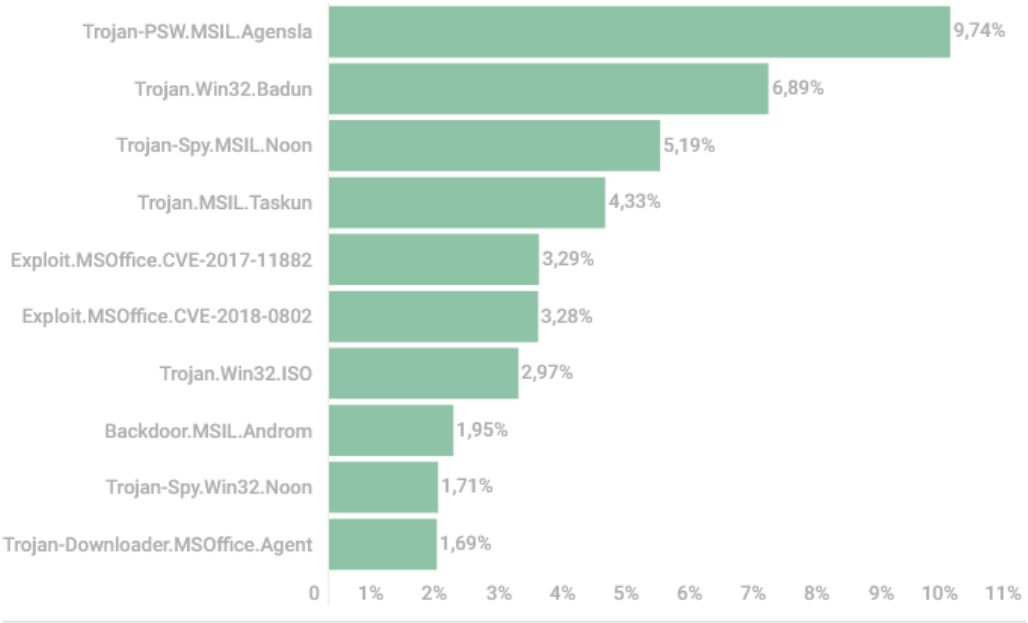


Fig. 3. Malware más comunes en el correo electrónico. [21]

La prioridad en el caso de presentarse algún correo electrónico sospechoso es evitar abrirlo ya que este puede contener malware incrustado o pueden afectar de manera económica a una persona o empresa, por lo que si llega a suceder este acontecimiento es necesario hacer las respectivas investigaciones informáticas forenses para tratar de encontrar en usuario, ip, puerto o algún tipo de indicio que pueda guiar al atacante.

EL proceso de análisis informático forense que aplicará a varios correos electrónicos cuya finalidad es hacer un daño a la persona que abra un enlace, descargue una imagen, un archivo, servirá para seleccionar un conjunto buenas prácticas proporcionadas por un estándar internacional que será elegido a través de una comparación entre varios estándares como (ISO 27001, NIST) que se analizará dentro de esta investigación.

La presente investigación tiene como objetivo informar a personas sobre los tipos de correos electrónicos de los que puede ser víctima, presentando su manera de operar y sus

diferentes presentaciones para que mediante las acciones seleccionadas se pueda moderar el acto de caer en este tipo de estafas o engaños a través de mensajería electrónica [2].

La adquisición de la información necesaria es sumamente relevante para proceder con la preservación de la evidencia identificando sus metadatos y demás elementos que caracterizan a los archivos digitales que se les ejecutará el análisis.

Por otra parte, en el proceso de análisis es necesario utilizar herramientas informáticas forense reconocidas y que tengan un buen grado de confiabilidad en sus resultados para así obtener un margen de error pequeño o nulo al momento de presentar el informe pericial final.

El actual proyecto de investigación está enfocado en el Plan denominado Creación de Oportunidades en el **Eje de Seguridad Integral.** [22]

- **Objetivo 9:** Garantizar la seguridad ciudadana, orden público y gestión de riesgos [22].
- **Política 9.1.** Fortalecer la protección interna, el mantenimiento y control del orden público, que permita prevenir y erradicar los delitos conexos y la violencia en todas sus formas, en convivencia con la ciudadanía en el territorio nacional y áreas jurisdiccionales [22].

1.5. ALCANCE DEL PROYECTO

El proyecto tiene dos fases, uno de que desarrollo a través de una investigación descriptiva, y otro mediante la experimentación. El primero consiste en determinar el nivel de exposición de ciberamenazas de los usuarios, y la segunda corresponde a la aplicación de métodos y técnicas de computación forense.

Para evaluar el nivel de exposición de las ciberamenazas se realiza una encuesta con el fin de conocer las habilidades respecto al uso y gestión de la seguridad de los correos electrónicos. Para ver formato de la encuesta (Ver Anexo 3).

Para la experimentación, se procedió a realizar un análisis de los tipos de correos electrónicos maliciosos para conocer su forma de operación, así como identificar los diferentes elementos que estos poseen para validar su integridad. La experimentación se desarrolla baja las siguientes etapas:

Fase 1: Adquisición. – Adquirir la evidencia digital a través de un repositorio en la nube para proceder al análisis siguiendo el protocolo dictado por el estándar UNE 71506:2013.

Fase 2: Preservación. – En esta fase mediante el uso de un software informático forense conocido como QFileHasher se verificará la autenticidad de cada uno de los correos electrónicos a analizar realizando una comparación de código hash de los correos electrónicos debido a que se necesita estar seguro de que los archivos a analizar son los correctos.

Fase 3: Análisis. – Uso de herramientas informáticas forense, para realizar procesos y tareas con la finalidad intentar dar una posible respuesta a preguntas que tienen relación con la investigación en curso.

Fase 4: Documentación. – Se procede a documentar en un formato de reporte informático forense el procedimiento realizado a la evidencia digital, herramientas utilizadas, métodos y demás desde que inicia el análisis hasta la generación del informe pericial siguiendo una secuencia temporal definida.

1.6. METODOLOGÍA DE INVESTIGACIÓN

1.6.1. Diseño de la investigación

Una investigación exploratoria se efectúa cuando no se han realizado investigaciones previas o existe poca información acerca del objeto de estudio [23]. Existe poca información acerca de la propuesta actual de carácter investigativo y práctico en el Ecuador, poco es el conocimiento de personas con relación a lo tecnológico enfocado a estos tipos de ataques o estafas. Por lo tanto, el objetivo es aplicar los conocimientos adquiridos en el transcurso de la carrera de T.I. para indagar respecto al tema.

Investigación Diagnóstica a través de la recolección de información mediante encuestas a personas sobre el uso de las buenas prácticas del estándar seleccionado cuando se haya realizado la comparación de estos.

Investigación Descriptiva es aquella que puede desarrollarse con un enfoque de carácter cualitativo para poder llegar a conocer las diferentes situaciones, costumbres y actitudes que se consideran predominantes a través de la descripción detallada de actividades, procesos y personas. [24]

Investigación practica experimental es aquella en donde se busca comprobar una hipótesis a través de la experimentación, observación directa o indirecta y por medio a de la experiencia [25]. En el caso del presente proyecto se obtendrá dichos resultados a través de los análisis forenses aplicados a los correos electrónicos.

1.6.2. Variables del estudio

Variable independiente: Ciberataques de correos electrónicos

Variable dependiente: Seguridad de datos personales

Hipótesis: La falta de información de cómo evitar ciberataques por correo electrónico compromete la seguridad de los datos personales.

A mayor desconocimiento de información sobre cómo evitar los ciberataques por correos electrónicos mayor inseguridad de los datos personales.

Explicación conceptual: Por medio de encuestas y prácticas se puede medir la frecuencia con el cual un grupo de personas es expuesto y cae en este tipo de ataques relacionados con correos electrónicos.

1.6.3. Población y muestra

La población objeto del estudio se tomó de una institución de educación básica-media ubicada en el cantón Santa Elena, de la provincia de Santa Elena. En este trabajo se consideró la totalidad de la población.

Tabla 1: Número total de población intervenida

Rango de edad	Género		Total
	Femenino	Masculino	
30 - 40	10	8	18
41 - 50	20	5	25
51 - 60	3	5	8
Más de 60	0	0	0
Total	33	18	51

1.6.4. Recolección y Procesamiento de la Información

1.6.4.1 Técnica de recolección de información

- **Técnica:** Encuestas y fuentes bibliográficas
- **Instrumento:** El cuestionario de preguntas serán dirigidas a un grupo de personas con el objetivo de conocer si el uso de las buenas prácticas elegidas fue de utilidad reduciendo así el impacto que los correos electrónicos falsos. Por otra parte, se utilizan bases de datos indexadas como Google Schoolar para acceder a los recursos bibliográficos que sirven como guía y análisis con relación a la problemática tratada en esta investigación.

1.6.4.2 Procesamiento de la información

El presente trabajo mostrará gráficos estadísticos de cada pregunta realizada de la encuesta dirigida a la población ya mencionada con anterioridad (Ver Anexo 3), con los resultados obtenidos se realizará una tabla de contingencia para comprender con mayor claridad los resultados obtenidos en esta investigación.

1.7. METODOLOGÍA DEL PROYECTO

1.7.1 Metodología UNE 71506:2013

La actual investigación se rige mediante el estándar UNE 71506:2013 que según una investigación [12], ésta es la mejor en comparación a otras debido a que reduce el tiempo en cuestión de procesos a realizar, las fases que posee son las siguientes:

Fig. 4. Metodología UNE 71506:2013

Según CloudFire, la seguridad y la privacidad no estaban integradas en un principio para los mensajes electrónicos y en la actualidad siguen sin estarlo, eso a pesar de la gran importancia que este mismo tiene como medio de comunicación personal e institucional dependiendo del ámbito a enfocarse[26]. Con relación a esto las amenazas de los correos

electrónicos se los clasificó en los siguientes: Fraude, Phishing, Malware Troyano, Apropiación de cuentas, ingeniería social, Malware.

Por otra parte, la revista que tiene como nombre “Barracuda” expone que la seguridad actual que poseen los servicios de correo electrónico no abastecen para las diferentes amenazas existentes y por existir[27]. Es así como la revista clasifica a las amenazas de correos electrónicos en 13 tipos ordenándolo del menos complejo al más complejo: correo no deseado, Malware, Extracción de datos, Suplantación de URL, Estafa, Suplantación de identidad personalizada, Suplantación de dominios, Falsificación de marcas, Chantaje, Fraude del correo electrónico empresarial, Secuestro de conversaciones, Suplantación de identidad lateral y Usurpación de cuentas.

Sin embargo, en la presente investigación se tomará y se analizará los 4 tipos de casos relacionados con los correos electrónicos son: Phishing, Apropiación de cuentas, Fraude y Malware

CAPITULO II. MARCO TEÓRICO

2.1. MARCO CONTEXTUAL

El presente trabajo está enfocado en el contexto académico. La información obtenida para esta investigación fue proporcionada por una institución de educación básica-media fundada en el año 1993 ubicada en la provincia de Santa Elena. La institución cuenta con un total de 51 docentes, y un total aproximado de 500 estudiantes distribuidos en jornadas matutina y vespertina. Para el estudio se consideró el total de la población docente, con quienes se evaluó el nivel de exposición de ciberamenazas a través de la aplicación de una encuesta.

2.1.1. Misión

La institución se propone a formar personas, con una educación integral, de calidad e innovadora, fomentando de esta manera los valores morales de justicia y de honestidad en los educandos.

2.1.2. Visión

Ofrecer una orientación de calidad, para que el estudiante pueda obtener una formación integra e innovadora, que permita ser personas de bien apegadas a los principios y valores.

2.2. MARCO TEÓRICO

2.2.1. Descripción de Seguridad informática y Malware

La informática, hace referencia al almacenamiento, tratamiento automatizado y transmisión de información, por medio de un hardware, software o redes de datos; tiene como objetivo que generen valor en los usuarios y que estos lo utilicen de la manera correcta según las características y restricciones de cada uno. Los elementos principales que se debe proteger en todo sistema de información es: hardware, software y la información, desafortunadamente, todos los elementos que conforman un sistema informático están expuestos a un ciberataque[28].

Teniendo en cuenta todo lo expuesto con anterioridad, se considera que la seguridad informática es definida como la mitigación de dichos riesgos a lo que se expone el sistema

informático, estos riesgos son amenazas y vulnerabilidades que pueden estar presentes por defecto en el dispositivo o por la poca intervención humana en estos.

2.2.2. Confiabilidad de las herramientas forenses en informática

Para la informática forense, existe un reto emergente relacionado con las herramientas tecnológicas que son utilizadas por los investigadores para avanzar considerablemente sus pericias. Por un lado, las herramientas que poseen licencia y son propiedad de una firma reconocida con relación al ámbito forense digital tienen un nicho de negocio que exige de los peritos una importante y fuerte inversión, tanto en herramientas de hardware y software[29].

Por otra parte, están la herramienta forense de código abierto, estas no son cuestionables en tribunales y poco se recomienda como herramienta de uso formal para presentar en audiencias debido a su condición.

2.2.3. El correo electrónico: herramienta que favorece la comunicación en el ámbito educativo.

La incorporación de la virtualidad en la vida cotidiana de las personas permitió nuevos campos de acción y servicios de educación, como por ejemplo la educación virtual, esta tiene los mismos principios que la educación presencial, por lo tanto, la educación virtual se mueve en lo real sustentado en formación integral y humana del sujeto. Por tal razón, analizar las interacciones académicas en los mensajes enviados por el facilitador o el estudiante a través del correo electrónico es fundamental para determinar fundamental, para determinar cómo los discursos orales se transforman en discursos con características de un texto escrito, con el fin de formular estrategias que potencialicen el uso del correo electrónico en el ámbito educativo desde lo escritural y lo humano[30].

Esto quiere decir que la comunicación mediatizada por ordenador (CMO) modifica no sólo las prácticas de enseñanza y aprendizaje, sino también las relaciones entre el que enseña y aprende; así mismo, replantea la práctica de lectura y escritura debido a las transformaciones lingüísticas y migración de la escritura impresa a la electrónica.

2.2.4 Ciberataques de correos electrónicos

Según la revisión bibliográfica se puede considerar que todo tipo de ciberataque es sancionado y penado por la constitución y demás leyes que rigen las comunicaciones a través del internet, por lo tanto, para el presente trabajo es necesario cuantificar los tipos de ciberataques en el contexto del actual proyecto.

La variable independiente "ciberataques a correos electrónicos" considerada para este proyecto, refleja de cierta manera el porcentaje de probabilidad de que una persona sea víctima de los diferentes tipos de ciberataques evaluados con anterioridad, por ejemplo: Correo electrónico zombie, Phishing, Estafa, Malware Troyano, Ingeniería Social y Malware.

2.2.5 Seguridad de datos personales

La huella digital de cada individuo es importante, motivo por el cual el nivel de protección de estas no debe de ser mínimo sino de carácter considerable para proteger la información personal y que esta misma no sea usado por ciberdelincuentes buscando un beneficio económico a través de actos delictivos.

La variable dependiente "Seguridad de datos personales" considera para este trabajo se verá afectada por el manejo y el uso de herramientas que aseguren la seguridad de las mismas, por lo que se considera que la utilización de este tipo de software es necesario en todo ámbito laboral.

2.3. MARCO CONCEPTUAL

2.3.1 Análisis informático forense

Se define como "Análisis informático forense" a la agrupación de técnicas de carácter científico y de análisis especializadas en las infraestructuras tecnológicas. A través de estas técnicas se tiene la posibilidad de realizar una identificación, preservación análisis y presentación de datos los mismos que tienen relevancia en cualquier proceso legal. Por lo que un análisis informático forense se lo ejecuto solo si se ha detectado una amenaza y que esta misma se haya materializado[31].

Por otra parte, el análisis permite evaluar las consecuencias producidas por el ataque realizado hacia una persona o empresa, así mismo a través de los procesos mencionados es posible crear un perfil del atacante utilizando la metodología SKRAM identificando las habilidades, conocimientos, recursos, autoridad y las motivaciones de este mismo[32].

2.3.1.1. Análisis Informático forense a correos electrónicos.

A través del análisis forense efectuado en un correo electrónico, es posible identificar una serie de datos pertenecientes al individuo atacante o ciberdelincuente que de alguna u otra manera logra vulnerar el derecho a la autodeterminación informativa de una persona[33].

La búsqueda, parametrización y reconstrucción de correos electrónicos es fundamental frente a casos relacionados con denuncias, engaños, estafas, amenazas u otro tipo de delito a través de este medio de comunicación. Es así como se pueden definir objetivos a alcanzar en este tipo de análisis como, por ejemplo: Analizar los riesgos y amenazas presentes en la manipulación de correos electrónicos. Definir los tipos de métodos y acciones que se empleará para que el correo electrónico tenga una validez legal. Por último, comprender la composición y el funcionamiento de cada uno de estos[34].

2.3.2. Estándar internacional

Un estándar internacional es un estándar técnico desarrollado por una o más organizaciones de estándares internacionales. Estos mismos están disponibles para su consideración y también para su uso alrededor del mundo. Se pueden utilizar de manera directa o lograr adaptarlo a las condiciones locales [35].

2.3.2.1 ISO 27000

ISO es considerada como una red que la conforman diferentes organismos internaciones de estandarización con alrededor de 160 países [36], es así que un ISO propone la utilización de un SGSI (Sistema de Gestión de Seguridad de la Información) que sirve para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección de los activos de información empresariales.

Fig. 5. Modelo de implementación según ISO 27001 [37]

Según ISO 27001 la implementación de un SGSI es una tarea importante para la mayoría de las organizaciones[38]. Sin embargo, si se hace de manera efectiva, existen beneficios significativos para aquellas organizaciones que dependen de la protección de información valiosa o sensible. Estos beneficios generalmente se dividen en tres áreas: comercial, tranquilidad y operacional.

Los riesgos en la seguridad de la información generalmente surgen debido a la presencia de amenazas para los activos que procesan, almacenan, mantienen, protegen o controlan el acceso a la información, lo que da lugar a incidentes [39]. El riesgo se gestiona mediante el diseño, implementación y mantenimiento de controles como ventanas bloqueadas, pruebas de software o la ubicación de equipos vulnerables por encima de la planta baja por lo que elaborar una adecuada gestión de riesgos que permita a las organizaciones conocer cuáles son las principales vulnerabilidades de sus activos de información.

ISO 27001 propone un modelo en ciclo denominado PHVA, el mismo que es conocido como ciclo Deming este puede aplicarse no solo al sistema de gestión. sino también a cada elemento individual para proporcionar un enfoque en la mejora continua. Es así como este estándar consta de 4 fases para la implementación: Planificar, hacer, verificar, actuar. Se puede observar de manera visual las fases propuestas por ISO 27001 [40].

- **Planificar:** Se define objetivos, recursos y requisitos del cliente, política organizativa e identificación de riesgos y oportunidades.
- **Hacer:** Implantar lo planificado

- **Verificar:** Controlar y medir los procesos para establecer el rendimiento de la política.
- **Actuar:** Tomar acciones para mejorar el rendimiento si este lo necesitase.

2.3.2.2 NIST

Las NIST es considerado como un marco que busca las mejoras de la seguridad informática en infraestructuras con un nivel de seguridad bajo, es conocida en inglés como "NIST Cibersecurity Framework", fue lanzada en Estados Unidos en el año 2014 por lo que en la actualidad se encuentra disponible en la versión 1.1 que fue liberada en el 2018. El objetivo del marco es ayudar a las pequeñas, medianas y grandes empresas a entender, gestionar y reducir riesgos informáticos y proteger su infraestructura de comunicación a través de un lenguaje común y brindando unas buenas prácticas de seguridad [41].

El Instituto Nacional de Estándares y tecnología (NIST) es una empresa no reguladore que incentiva a la innovación a través del uso de herramientas científicas, estándares internacionales y tecnología de medición. El marco de ciberseguridad que es presentado por este ente consta de estándares, pautas y buenas prácticas que impulsan a las empresas a mejorar el proceso de gestión de riesgo que se lleva a cabo. El diseño de este framework posee una flexibilidad que da la posibilidad de integrarse a los procesos de seguridad ya existentes en una empresa [42].

La implementación de las normas NIST en una empresa puede ser beneficioso a continuación se describen los beneficios de utilizar este estándar internacional en un ambiente empresarial. La primera ventaja es que describe la situación inicial que tiene la empresa en el ámbito de seguridad informática, para luego identificar y darles prioridad a las oportunidades de mejora presente en un contexto continuo y repetible[43].

El presente marco se encuentra organizado en cinco funciones claves: identificar, proteger, detectar, recuperar. Son 5 términos que son conocidos, cuando estos son considerados en conjuntos pueden llegar a proporcionar una visión integral del ciclo de vida para la gestión de ciberataques [44].

El uso de NIST se centra en ayudar a la empresa mediante buenas prácticas en el ambiente laboral y es así como se definen 5 áreas que se pueden implementar para el correcto uso de este estándar internacional [45].

- **Identificación:** Se elabora un listado del hardware y el software que posee la empresa y sus políticas de protección a estos dispositivos.
- **Protección:** Control de acceso a los dispositivos informáticos, se codifican datos, creación de copias de seguridad.
- **Detección:** Monitoreo de personal que ingresa a áreas no autorizadas, investigación de la red para encontrar actividad sospechosa.
- **Respuesta:** Notificación a clientes, empleados y demás personas que pueden llegar a comprometer sus datos personales, actualizar las políticas de ciberseguridad a través de la experiencia.
- **Recuperación:** Reparación y análisis de los equipos informáticos afectados para comprobar el estado de infección y solucionar el problema.

2.2.3 Correo electrónico

El correo electrónico es conocido como el método de comunicación e interacción que utilizad dispositivos electrónicos para el envío y recepción de mensajes a través de redes informáticas. Este medio de comunicación es reconocido como uno de los más populares, sin embargo, la prevalencia y vulnerabilidades de este mismo lo convierten en un blanco de ciberataques[46].

El correo electrónico es un medio para intercambiar información por lo que la poca seguridad que existe da la posibilidad a que un atacante pueda interceptar un mensaje no cifrado, propagar algún virus o realizar phishing a través de ingeniería social o suplantación de identidad.

2.3.3.1. Ciberataques a correos electrónicos

2.3.3.1.1. Phishing

El phishing rata sobre el envío de correos electrónicos que simulan proceder de fuentes de confianza tales como: bancos, compañías reconocidas públicas o privadas, sin

embargo, su principal objetivo es manipular al receptor del mensaje para robar información personal o empresarial [47].

Fig.6. Frases típicas presentadas en un Phishing [47]

2.3.3.1.2. Zombie o apropiación de cuentas

Es un ataque informático a correos electrónicos que consiste en robar la identidad digital de una persona, alguien ajeno a la cuenta ingresa de manera ilegal a la cuenta de una víctima para obtener diferentes beneficios cambiando detalles de la cuenta, realizando compras, o replicando un mensaje de correo electrónico malicioso[48]. Existen diferentes señales para identificar que se está tratando de realizar este tipo de ataque, una de las señales es el exceso de ingresos fallidos a una cuenta, sin embargo, también pueden obtener acceso a una cuenta de correo electrónico por medio de un código incrustado en un mensaje de correo electrónico, imagen, video o documento.

2.3.3.1.3. Amenazas o Engaños

Es un tipo de estafa, también es conocida como phishing textual el cual se dirige a las víctimas potenciales mediante el envió de un mensaje de correo electrónico. Lo común de este tipo de ciberataques es que suelen prometer alguna recompensa, dinero gratis o otros incentivos a cambio de información personal o bien pueden tratarse de amenazas con el fin de hacer asustar y desesperar a la víctima por medio del uso de ingeniería social.

2.3.3.1.4. Malware

Estos tipos de correos electrónicos contienen archivos adjuntos, estos pueden ser documentos, videos, imágenes y demás archivos que puedan contener algún malware e infectar a las posibles víctimas[48]. Este software utilizado en los correos electrónicos es utilizado con varias finalidades, ejemplo de estas finalidades son: robar información, tomar el control de sistemas o realizar ataques DOS.

2.3.3.1.5. Etiquetas de un correo electrónico.

Los correos electrónicos poseen varias etiquetas, estas indican información detallada sobre el envío del correo electrónico, saltos, contenido y demás información relevante para la investigación realizada. Para más información revisar el Anexo 2 (Ver Anexo 2).

2.2.3.3. Papel de los correos electrónicos en el proceso judicial.

Los correos electrónicos son considerados como prueba de hechos en multitud de procesos judiciales de todos los órdenes, en especial en las áreas del ámbito laboral, civil y mercantil. Es verdad que los correos electrónicos fueron diseñados para la comunicación, sin embargo, no se diseñaron para certificarse por si mismo la autenticidad de la comunicación efectuada[49]. Por todo aquello mencionado anteriormente, es necesario que un perito informático certificado realice un peritaje de correos electrónicos para comprobar su veracidad y así presentarlo en diferentes procesos judiciales.

2.2.4. Protocolos

El protocolo es considerado como un conjunto de normas para formatos de transmisión de datos y procedimientos que permiten que los diferentes dispositivos electrónicos y software puedan intercambiar información y se establezca una comunicación eficiente. Cada dispositivo que conforma un sistema de comunicación debe de seguir los protocolos ya establecidos para que así se pueda interpretar la información enviada o recibida[50].

También son consideradas como reglas o normas que son elaboradas para garantizar la confidencialidad, integridad y disponibilidad de la información y de la comunicación entre dispositivos. Por lo tanto se puede decir que son medidas de seguridad personas externas o ajenas a un entorno de comunicación no pueda manipular, interceptar o destruir la información transmitida[51].

2.2.4.1. Protocolo POP3

Se lo conoce como el protocolo de comunicaciones más extendido para poder leer un correo electrónico, conocido por sus siglas POP3 (Post Office Protocol). Las cuentas de correo electrónico que poseen dicho protocolo cuentan con ciertas ventajas entre ellas están: La descarga de toda la información en el disco duro del cliente para que de esta manera el servidor que provee el servicio de mensajería no retenga copia de mensajes [52].

Fig.7. Protocolo PoP3 [52]

2.2.4.1. Protocolo IMAP

El protocolo IMAP (Internet Message Access Protocol) permite obtener el acceso a los correos electrónicos que se encuentran almacenados en un servidos, es decir, que estos se pueden visualizar desde cualquier dispositivo que posea conexión a internet, sin embargo, hay que recalcar que el protocolo mencionado sirve para visualizar mensajes y no es un protocolo de envió de emails[53].

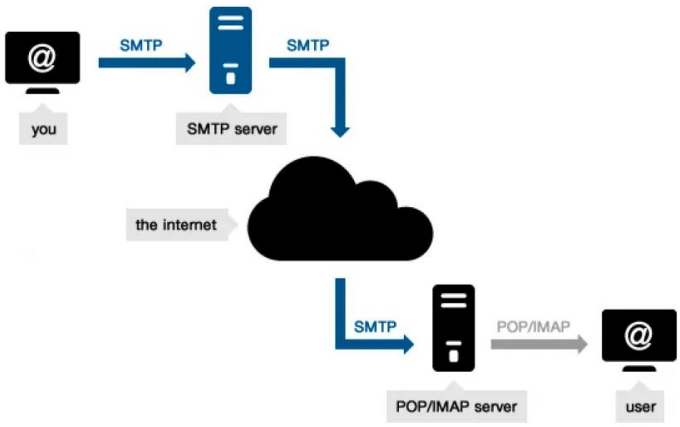
Cuando se procede a leer un mensaje de correo mediante el protocolo IMAP, este no se descarga ni se almacena en el equipo, lo que en realidad está sucediendo es que se visualizado desde un servidor de correo electrónico que podría estar ubicado en cualquier parte del mundo[54].

Fig.8. Protocolo IMAP [54]

2.2.4.1. Protocolo SMTP

EL protocolo SMTP es considerado como un protocolo de transferencia de correo electrónico TCP/IP, este es utilizado para enviar y recibir este tipo de información, este se puede utilizar junto con el POP3 o IMAP para poder guardar mensajes en un servidor de correo electrónico para luego descargarlo cuando se lo requieran [55].

Además, permite la accesibilidad de la información a través del envío y recibo de esta misma esto de manera indiferente si poseen un software o hardware distinto. El protocolo estandariza la forma en que el correo electrónico viaja hasta el destino indicado, dando la posibilidad de una entrega correcta y eficiente [56].



Fig,9. Protocolo SMTP. [55]

2.2.5 Comunicación en el correo electrónico

En una comunicación realizada a través de correo electrónico existen diversas partes a considerar, lo cual es conformado por: emisor, receptor, agente de usuario del emisor (UA), UA del receptor, agente de transferencia de correo (MTA) del emisor y MTA del receptor. Se pueden dar los casos en que es necesario el MTA de otras partes para llegar al destino. La UA es la plataforma que usan los usuarios de correo electrónico para enviar/recibir mensajes electrónicos (Outlook, Gmail, etc.), por otra parte, el MTA es el servidor de correo electrónico. En la mayoría de los casos, el emisor y el receptor tienen el control del UA. Existen diferentes opciones de configuración a establecer e inciden en la seguridad y privacidad de las comunicaciones a través de esta plataforma, cifrado extremo a extremo, TLS implícito o explícito y demás. Sin embargo, los usuarios finales

poseen conocimientos acerca los estándares de seguridad que usan los proveedores de correo electrónico al enviar y recibir emails [57].

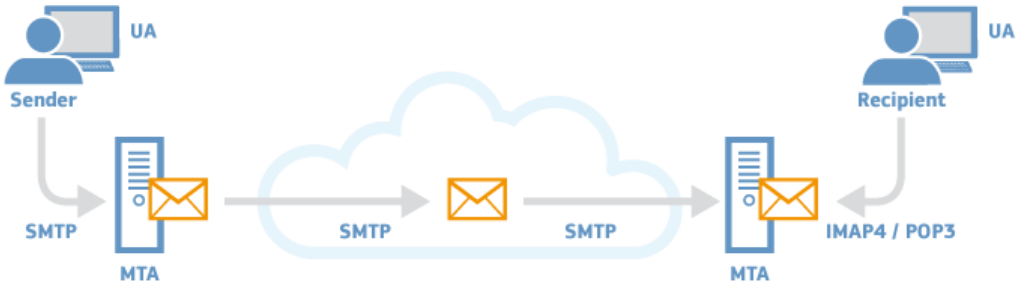


Fig.10. Comunicación en el correo electrónico

2.2.6. Intervención del atacante

2.2.6.1. Ataque a la confidencialidad de un correo electrónico

El sistema de correo electrónico considera que todos los agentes que intervienen dentro de la comunicación son seguros y confiables, cabe recalcar que esto incluye a la red de comunicación. Sin embargo, cuando existe una comunicación entre servidores SMTP y esta se realiza a través del internet, la información que viaja puede ser interceptada por algún agente externo. Por lo que la ausencia de protocolos de seguridad permite que este tipo de actos se lleven a cabo y la comunicación no podría ser privada como se cree. El objetivo es poder observar toda la información de un canal de comunicación sin autorización de los 2 actores principales, es difícil de detectar debido a que no existe manipulación de la información que se transmite, solo es una visualización y en otros casos una copia de la misma [58].

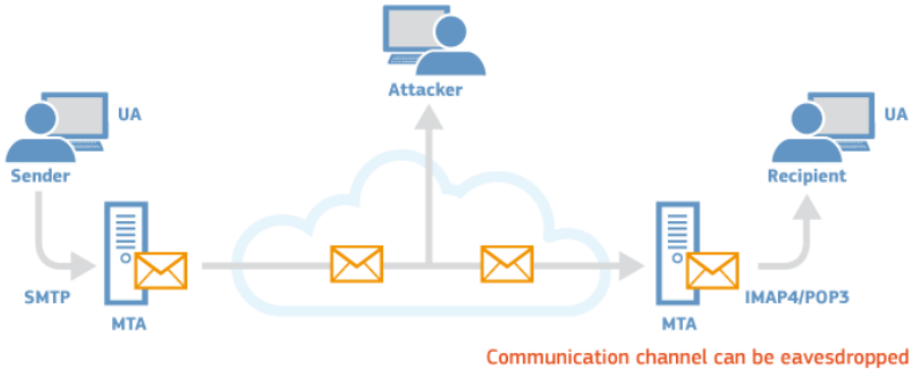


Fig.11. Ataque a la confidencialidad [58]

2.2.6.1. Ataque a la identidad del emisor del correo electrónico

El ataque a la identidad del emisor del correo electrónico o robo de identidad es una de las principales vulnerabilidades que están presentes en este servicio de comunicación y en la mayoría de los casos el usuario al que se le robó la información no se dará cuenta y es considerado como uno de los más difíciles de detectar, sin embargo, mediante la información de que está presente en la cabecera de cada mensaje de correo electrónico se puede detectar. Los atacantes ocultan la información a través de una técnica llamada spoofing que consiste en tomar una dirección de correo electrónico cualquiera y sustituirla por una aparentemente de confianza y segura[59].

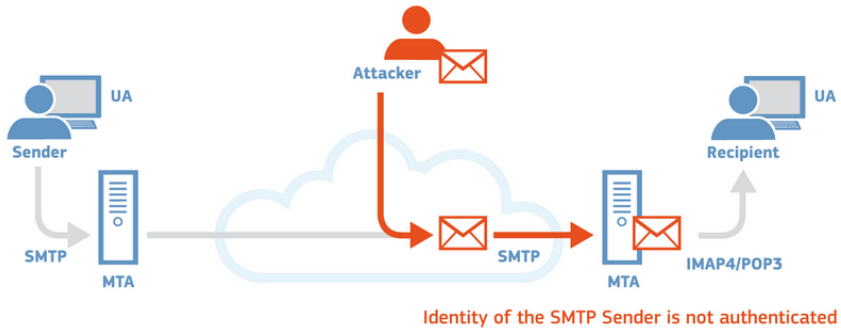


Fig.12. Ataque a la identidad del emisor. [59]

2.2.6.1. Ataque a la integridad de los mensajes

El ciberdelincuente se aprovecha de la falta de estándares de seguridad que intervienen la comunicación entre 2 personas para así modificar el contenido de los correos electrónicos que se envían, esto se lo puede realizar con el contenido del correo electrónico, así como a los archivos adjuntos en este, este escenario se puede prevenir o reducir el riesgo siempre y cuando se envíen mensajes cifrados con un algoritmo de codificación confiable[60].

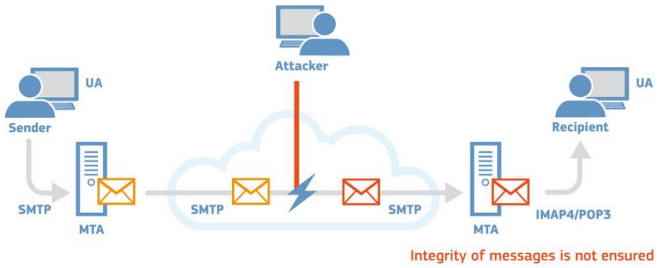


Fig.13. Ataque a la integridad de mensajes electrónicos. [60]

2.4. MARCO LEGAL

2.4.1. Código Orgánico Integral Penal (COIP)

El COIP publicado en el Registro Oficial Suplemento N°180 del 10 de febrero de 2014, se caracteriza por ser sistemático, preciso y claro, lo mismo que facilita la certeza perceptiva. Además, se compone de parte material, formal y de ejecución, el cual fue el producto de la necesidad de innovar y especializar las diferentes normas existentes en ese entonces para adaptarlas a los cambios sociales y la realidad actual, formando la manera de concebir el Derecho y de razonar lo jurídico[61].

Art. 103.- Pornografía con utilización de niñas, niños o adolescentes.

Art. 173.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.

Art 178.- Violación a la intimidad.

Art. 179.- Revelación de secreto.

Art. 186.- Estafa.

Art. 190.- Apropiación fraudulenta por medios electrónicos.

Art. 229. - Revelación ilegal de información de bases de datos

Art. 230.- Interceptación ilegal de datos

Art. 231.- Transferencia electrónica de activo patrimonial

Art. 232.- Ataque a la integridad de sistemas informáticos.

Art. 234. - Acceso no consentido a un sistema informático, telemático o de telecomunicaciones

Art. 354.- Espionaje.

Art. 456.- Cadena de custodia.

Art. 475.- Retención de correspondencia.

Art. 476.- Interceptación de las comunicaciones o datos informáticos.

2.4.2. Ley Orgánica de Protección de Datos Personales

Este reglamento tiene como finalidad garantizar el ejercicio del derecho a la protección de datos personales, el mismo que incluye el acceso y decisión sobre la información y datos de este carácter, así como su correspondiente protección. Para dicha acción regula, prevé y se desarrolla principios, derechos, obligaciones y mecanismos de tutela[62].

Art. 5.- Integrantes del sistema de protección de datos personales.

Art. 8.- Consentimiento.

Art. 25.- Categorías especiales de datos personales.

Art. 36.- Excepciones de consentimiento para la transferencia o comunicación de datos personales.

Art. 37.- Seguridad de datos personales.

Art. 40.- Análisis de riesgo, amenazas y vulnerabilidades.

Art. 41.- Determinación de medidas de seguridad aplicables.

Art. 65.- Medidas correctivas.

Art. 70.- Infracciones graves del Encargado de protección de datos.

Art. 75.- Autoridad de protección de datos personales

Art. 76.- Funciones atribuciones y facultades.

2.4.3. Ley de comercio electrónico, firmas y mensajes de datos.

El uso de sistemas de información y de redes informáticas, incluido la navegación por internet, ha adquirido importancia para el progreso y desarrollo del comercio y la producción, lo cual permite la realización y concreción de múltiples negocios de transcendental importancia, tanto así en el ámbito público como el privado. Por lo que es necesario impulsar el acceso de la población ecuatoriana a los servicios electrónicos que son generados a través de medios electrónicos [63].

Art. 2. – Reconocimiento jurídico de los mensajes de datos.

Art. 3. – Incorporación por remisión.

Art. 5. – Confidencialidad y reserva.

Art. 6. – Información escrita.

Art. 7. – Información original.

Art. 8. – Conservación de mensajes de datos.

Art. 9. – Protección de datos.

Art. 10. – Procedencia e identidad de un mensaje de datos.

Art. 11. – Envió y recepción de los mensajes de datos.

Art. 12. – Duplicación de mensajes de datos.

Art. 16. – Firma electrónica en un mensaje de datos.

Art. 32. – Protección de datos por parte de las entidades de certificación de información acreditadas.

Art. 48. – Consentimiento para aceptar mensajes de datos.

Art. 57. – Infracciones informáticas.

CAPITULO III PROPUESTA

El presente capítulo describe el análisis de la integridad de los correos electrónicos, y sus respectivos resultados, mediante el desarrollo de cada una de las fases detalladas en el apartado de la metodología.

3.1. ADQUISICIÓN

El proceso técnico para obtener el hash se describe en el número de anexo que corresponde a cada caso.

Tabla II: Adquisición de correos electrónicos

N° de Caso	Tipo de Ciberataque	Origen de la evidencia	Descripción del incidente	N° Anexo
1	Email Zombie o Apropiación de cuentas	Evidencia extraída desde el dominio upse a través de la cuenta lhaz@upse.edu.ec	El ciberataque consiste en que la víctima descargue un malware que hace reenviar el mismo mensaje a su lista de contactos replicando el malware incrustado.	**(Ver Anexo 4)**
2	Phishing	Evidencia extraída de un correo electrónico personal (cruzlourdes@hotmail.es)	Consiste en que la víctima piense que es un correo electrónico verídico de la institución bancaria que maneja, sin embargo, el objetivo de este correo electrónico la persona proporcione sus datos personales como: Correo electrónico, contraseña, pin de seguridad y demás información que permita al atacante acceder a la cuenta bancaria.	**(Ver Anexo 5)**

3	Fraudulento o Engaño	Evidencia extraída desde un correo electrónico personal lidice_haz@hotmail.com	El ciberataque tiene como finalidad hacer que su víctima se comunique con una persona y así cumplir con sus demandas, en este caso se adjunta una supuesta carta de remitente una institución reconocida como lo es la INTERPOL, el objetivo es que mediante técnicas de engaños la víctima pueda sucumbir al miedo o temor de este mismo mensaje.	**(Ver Anexo 6)**
4	Malware	Evidencia extraída desde un correo electrónico personal victoria.haz@hotmail.com	El actual caso consiste en que el atacante adjunta un documento, supuestamente se trata de una factura de la víctima, así mismo escribe un mensaje detallando que pide disculpas por la demora de la generación del documento, el objetivo es que por curiosidad la persona abra el documento adjunto en este correo electrónico para así infectar su equipo.	**(Ver Anexo 7)**
5	Ingeniería Social	Evidencia extraída desde un correo electrónico personal renzonqc@gmail.com	El ciberataque consiste en que la víctima ingrese en el enlace adjunto, dentro del cuerpo de este correo electrónico se puede observar una imagen en donde se ofrece un seguro de autos confiable y económico, esta imagen sirve para que la víctima	**(Ver Anexo 8)**

			se interese en lo que se está ofreciendo. Como dato adicional, el correo electrónico recibido posee la misma foto de la víctima y un número, se desconoce el objetivo o finalidad de este mismo.	
6	Malware	Evidencia extraída desde un correo electrónico personal lidice_haz@hotmail.com	En el caso actual se tiene como novedad que el correo electrónico presenta un mensaje, afirmando que la víctima ha sido acreedora de un valor monetario, sin embargo, además de esto se encuentra un archivo adjunto con extensión html en donde supuestamente se encuentra pasó para completar el proceso mencionado anteriormente.	**(Ver Anexo 9)**

3.2. PRESERVACIÓN

Generación de código Hash

En la presente fase se procede a descargar los correos electrónicos con su extensión eml, los mismos que serán usados para generar su código hash y por consiguiente realizar el análisis de la estructura que estos poseen. Mediante el código hash se puede verificar la veracidad de un archivo, por lo que también es importante realizarlo dentro de la investigación en cuestión. Con el software QFileHasher se debe de localizar los archivos de correos electrónicos ya descargados para proceder con la generación del código.

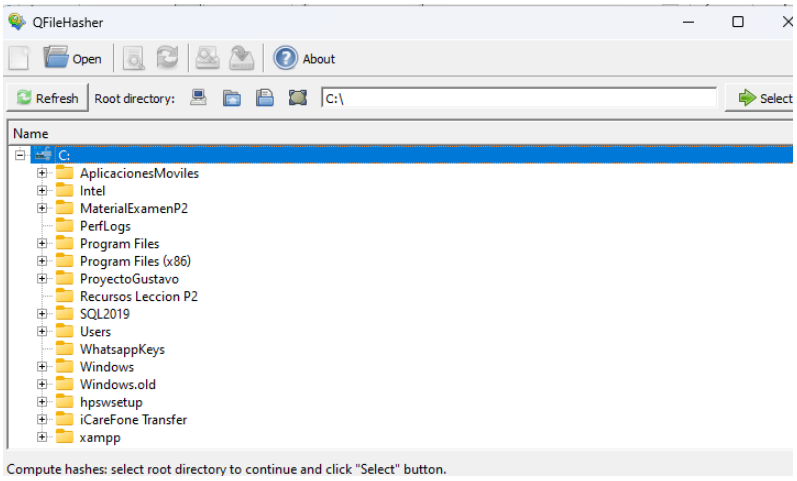


Fig.14. Interfaz del Software QFileHasher

Cuando se localiza el archivo se procede a abrirlo en el software en cuestión para así generar el código que permite saber la confiabilidad de un archivo, dando, así como resultado los códigos hash de cada uno de los archivos procesados en el software.

Para la creación de cada uno de los códigos hash es necesario seleccionar el documento requerido y presionar el botón “Start”, el mismo que permitirá obtener la información requerida para proseguir con las siguientes fases. El proceso técnico para obtener el hash se describe en el número de anexo que corresponde a cada caso.

Tabla III: Código hash para cada caso

N° de Casos	Tipo de Ciberataque	Ip Origen	Hash Sha1	N° Anexo
1	Zombie	10.173.99.22	5913293ccad547840a07f72f9b2d5f890db80e0b	**(Ver Anexo 4)**
2	Phishing	10.13.6.249	a2b457679c20be90f411b7c0e2dd61b1	**(Ver Anexo 5)**
3	Estafa o Engaños	209.85.221.45	f3c9f671d09b0ecd4fcbf87dbca973b9baa39305	**(Ver Anexo 6)**

4	Malware	208.13.21.10	22840df8e8843cd4b9b1fbcf04864b0b27ac168c	**(Ver Anexo 7)**
5	Ingeniería social	209.85.220.101	8300eae3435bc2caf249d7eab994a887a6e8ea1e	**(Ver Anexo 8)**
6	Malware	10.152.24.234	dfc4592df5b5d0a85f888b0426ba4ee2676a86e0	**(Ver Anexo 9)**

3.3. ANÁLISIS

Una vez adquirida la información y de asegurarse de que la evidencia en cuestión fue preservada, el siguiente paso es realizar su análisis para identificar huellas digitales de los posibles atacantes, en este procedimiento es importante el uso del software forense propuesto en la investigación para el correcto estudio e identificación de: credencias, usuario, correo electrónico, ip y demás datos que revelen la identidad del atacante.

El siguiente procedimiento sirve para cargar los archivos con extensión eml a analizar, es importante recalcar que este procedimiento es el mismo para todos los tipos de correos electrónicos maliciosos por analizar:

1. Para cargar el archivo de extensión eml es necesario abrir el software AccesData FTK Imager, el mismo que permitirá analizar la estructura de este email malicioso, en la siguiente figura se puede observar el entorno del software antes mencionado.

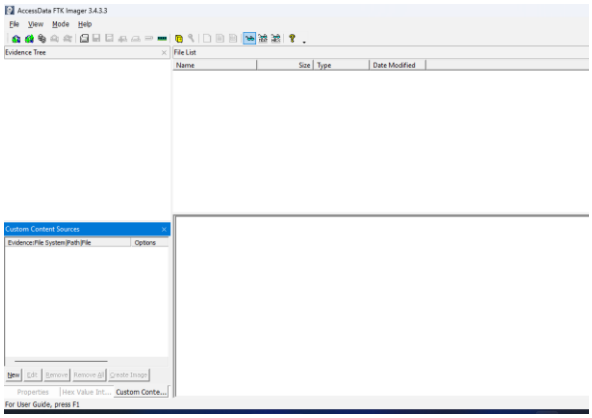


Fig.15. Entorno de trabajo de AccessData FTK Imager

2. Para abrir el archivo eml es necesario dirigirse a la parte superior izquierda y encontrar la opción de “File” para luego seleccionar la opción “Add Evidence Item” tal y como se puede observar en el siguiente gráfico.

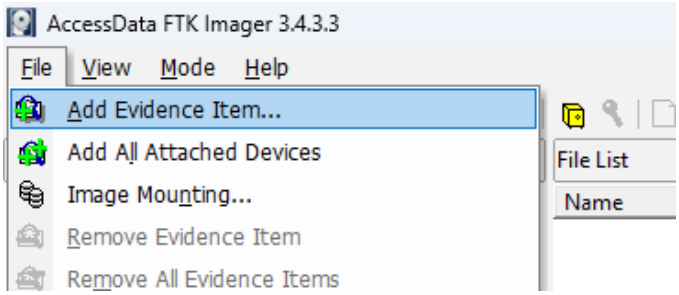


Fig.16. Opciones para cargar archivos dentro del software Ftk Imager.

3. Cuando se abra la ventana se selecciona la opción de “Contents of a folder” siguiente figura, después dar al botón de Siguiente en donde se abrirá otra ventana en donde es necesario escribir o seleccionar la ruta de la carpeta en donde se encuentra toda la evidencia digital a analizar.

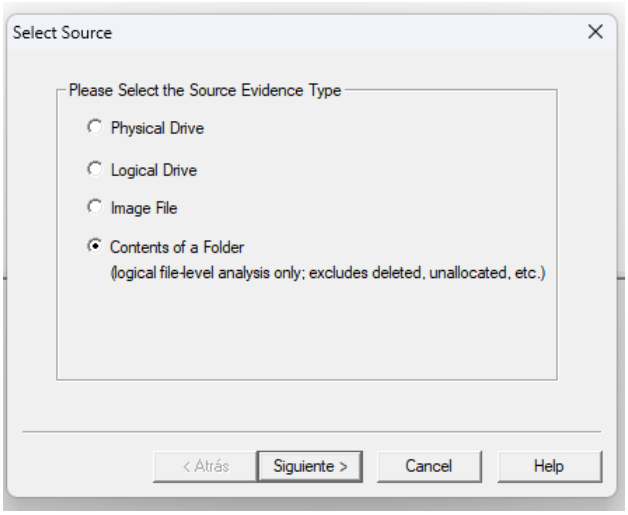


Fig.17. Ventana de Select Source

4. Se selecciona la ubicación de la carpeta en donde se encuentra la evidencia, en este caso la evidencia se encuentra localizada en la siguiente ruta: C:\Users\renzo\OneDrive - Universidad Península de Santa Elena\Escritorio\Universidad\2022-2\Integracion curricular\emails-forense, una vez seleccionado se da clic en el botón finalizar.

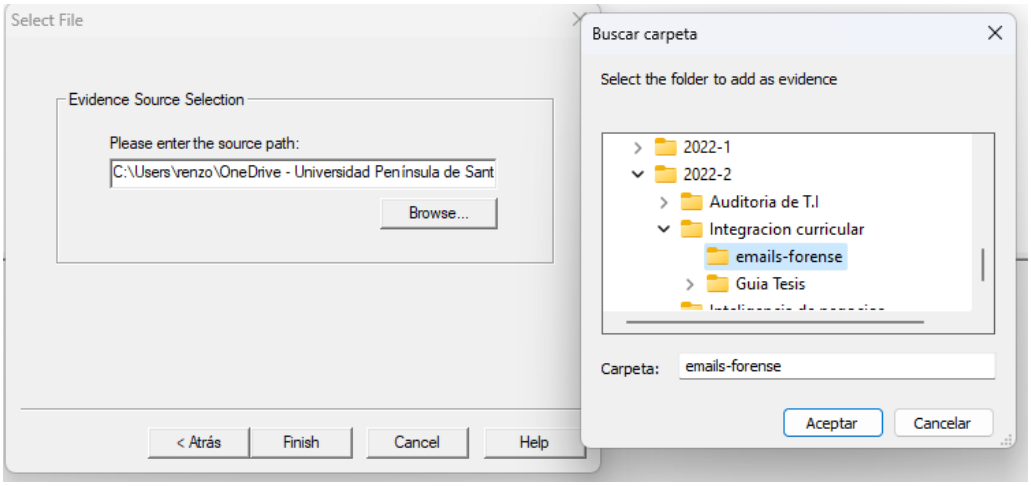


Fig.18. Ventana de Select Source

5. En la parte izquierda de la interfaz del software aparece un apartado denominado "Evidence Tree", en donde se encuentra cargada la información relevante para la investigación actual, lo mencionado anteriormente se lo puede visualiza.

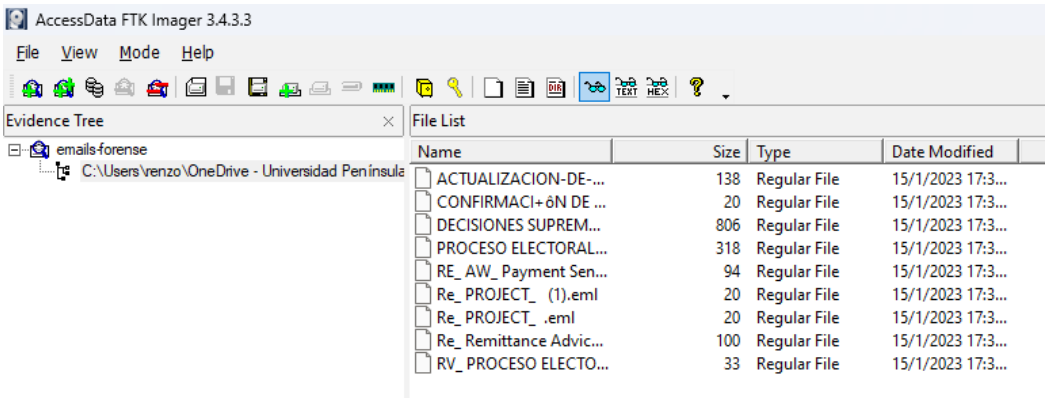


Fig.19. Información a analizar cargada

Es esencial tener un conocimiento previo sobre las etiquetas presentes dentro de la estructura de un correo electrónico, es por eso necesario visualizar el Anexo 2 (Ver Anexo 2), en donde se expone la definición de cada una, esto debido a que la investigación solo tomará en cuenta las necesarias para identificar las huellas digitales de los posibles delincuentes.

3.3.1 Caso 1 (Zombie).

El archivo relacionado con el ejemplo a tratar en este punto es aquel denominado como "PROCESO ELECTORAL.eml", el mismo que posee un archivo adjunto el cual incrusta un programa maligno para apropiarse del correo electrónico y así reenviar un mensaje electrónico a todos los miembros de su lista de contactos.

Para acceder a la estructura de un archivo eml en el software AccessData se debe seleccionar el documento que posee la información que se requiere analizar.

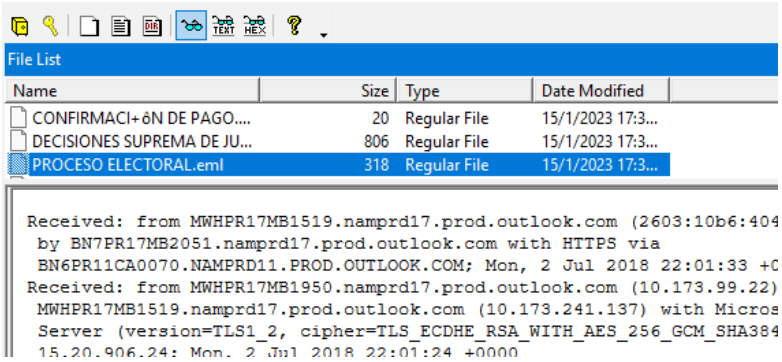


Fig.20. Información del archivo "PROCESO ELECTORAL.eml"

Tabla IV: Análisis Caso 1

ANÁLISIS DE CABECERA			
(Ver Anexo 4)			
ETIQUETAS	**DESCRIPCIÓN**	**RESULTADOS**	**OBSERVACIÓN**
Received	La observación "Received" se repite 4 veces, eso representa a los diferentes saltos que el mensaje electrónico dio antes de llegar a la bandeja de entrada de la víctima.	Se aprecia que la cantidad de saltos en total son 4. Con las siguientes IP: 10.173.99.22 10.173.241.137 10.173.104.15	El punto de origen es la dirección IP 10.173.99.22.

From	Esta etiqueta presenta información de la cuenta que emite el correo electrónico, en este caso es: “rectorado@upse.edu.ec”	La dirección de correo electrónico presente en esta etiqueta está asociada con UPSE.	Dado a un análisis de la información proporcionado se presume que fue manipulado para enviar el comunicado adjunto.
To	La etiqueta mencionada presenta a las cuentas llegó la información del correo electrónico infectado.	Se aprecia que el atacante dirige el su acto a personas pertenecientes a la institución	
ANALISIS DE CUERPO DE MENSAJE			
ETIQUETAS	**DESCRIPCIÓN**	**RESULTADOS**	**OBSERVACIÓN**
Content	En el correo electrónico presenta una escritura formal simulando ser enviado por una autoridad que maneja la cuenta asociada el caso 1	Mediante la comparación con un correo electrónico enviado desde la misma universidad se nota la diferente en el uso de tipografía.	El correo electrónico a través del comunicado que adjunto tiene como objetivo hacer que estudiantes y trabajadores de la institución abran el archivo y se infecten.
ANÁLISIS DE ARCHIVOS ADJUNTOS			

NOMBRE DEL ARCHIVO	DESCRIPCIÓN	RESULTADOS	OBSERVACIÓN
Oficio N 260.pdf	Debido al contexto proporcionado por el correo electrónico, el archivo simula ser un oficio enviado por la institución.	El análisis del archivo con el nombre especificado da como resultado de que es seguro según la fuente de Virus Total	Ya que el análisis del archivo dio como resultado que es seguro por abrirlo, lo que se puede apreciar dentro de este es que el oficio adjuntado por la institución fue escaneado y enviado a varios departamentos de la universidad.
Full_transaction_info-66.zip	Archivo con extensión tipo zip, el mensaje no informa nada sobre lo que podría contener este documento adjunto.	El análisis realiza da como resultado de que este archivo se encuentra infectado por varios malwares incrustados.	Este archivo posee virus de diferentes tipos entre esos se encuentran: 4 tipos de virus troyanos embebidos.

3.3.2 Caso 2 (Phishing).

El archivo relacionado con el ejemplo a tratar en este punto es aquel denominado como “BLOQUEAMOS TU CUENTA.eml”, el mismo que posee el método de ingeniería social para que la víctima ingrese a la página que está etiquetada como phishing.

Para acceder a la estructura del presente caso en el software AccessData se debe seleccionar el documento que posee la información que se requiere analizar.

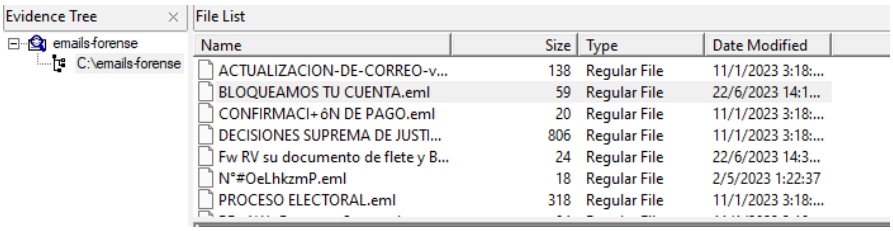


Fig.21. Información del archivo "BLOQUEAMOS TU CUENTA.eml"

Tabla V: Análisis Caso 2

ANÁLISIS DE CABECERA			
(Ver Anexo 5)			
ETIQUETAS	**DESCRIPCIÓN**	**RESULTADOS**	**OBSERVACIÓN**
Received	La observación "Received" se repite 6 veces, eso representa a los diferentes saltos que el mensaje electrónico dio antes de llegar a la bandeja de entrada de la víctima.	Se aprecia que la cantidad de saltos en total son 6. Sin embargo, a través del análisis de pudo obtener 2 direcciones IP: 40.92.97.75 10.13.6.249	El punto de origen es la dirección IP 40.92.97.75
From	Esta etiqueta presenta información de la cuenta que emite el correo electrónico, en este caso es: "yolissa-4@hotmail.com"	La dirección de correo electrónico presente en esta etiqueta es considerada como una dirección de	El correo electrónico fue enviado a través del correo electrónico antes mencionado, sin embargo,

		correo electrónico personal.	aparentemente el remitente es el banco pichincha
To	La etiqueta mencionada presenta al receptor de la información del correo electrónico phishing.	Se aprecia que el atacante dirige el su acto a una sola persona con la siguiente dirección de correo electrónico: cruzlourdes@hotmail.es	Se presume que el ataque fue solo a esa persona debido a que en la etiqueta TO no existe una lista de receptores del mensaje como aparece en el caso anterior.
ANALISIS DE CUERPO DE MENSAJE			
ETIQUETAS	**DESCRIPCIÓN**	**RESULTADOS**	**OBSERVACIÓN**
Content	En el correo electrónico presenta un supuesto comunicado del banco indicando que es necesario realizar un login en la página porque la cuenta de la persona fue bloqueada.	Mediante la comparación con un correo electrónico de parte de la institución bancaría se puede determinar el intento de plagiar sus comunicados además de que estos comunicados poseen aviso tal como: “El banco no de pedirá	El correo electrónico a través del comunicado que adjunto tiene como objetivo hacer que la víctima ceda al miedo de perder su cuenta o dinero en la institución bancaria.

		información personal como usuarios y contraseñas".	
ANÁLISIS DE PÁGINA WEB			
NOMBRE DEL ARCHIVO	**DESCRIPCIÓN**	**RESULTADOS**	**OBSERVACIÓN**
Phishing Banco Pichincha	Es una copia idéntica a la página oficial, sin embargo, existen ciertos detalles importantes a destacar para identificar sus diferencias.	Mediante el análisis realizado con VirusTotal da como resultado que efectivamente es una página de categoría phishing, la url, y pequeños detalles en el login del phishing lo delatan.	Antes de ingresar a la página phishing el navegador la reconoce como tal, es por eso que se necesita seguir las instrucciones y evitar páginas de dudosa procedencia.

3.3.3 Caso 3 (Fraude o engaño).

El archivo relacionado con el ejemplo a tratar en este punto es aquel denominado como "DESICIONES SUPREMA DE JUSTICIA EN SU CONTRA.eml", el mismo que posee el método de ingeniería social para que la víctima se ponga en contacto con el remitente de este correo electrónico.

Para acceder a la estructura del presente caso en el software AccessData se debe seleccionar el documento que posee la información que se requiere analizar.

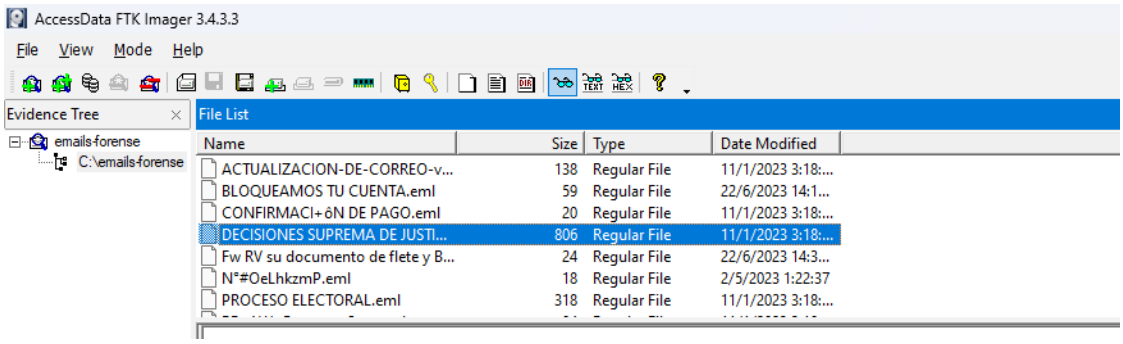


Fig.22. Información del archivo "DESICIONES SUPREMA DE JUSTICIA EN SU CONTRA.eml"

Tabla VI: Análisis Caso 3

ANÁLISIS DE CABECERA			
(Ver Anexo 6)			
ETIQUETAS	**DESCRIPCIÓN**	**RESULTADOS**	**OBSERVACIÓN**
Received	La observación "Received" se repite 5 veces, eso representa a los diferentes saltos que el mensaje electrónico dio antes de llegar a la bandeja de entrada de la víctima.	Se aprecia que la cantidad de saltos en total son 5. Sin embargo, a través del análisis de pudo obtener 3 direcciones IP: 209.85.221.45 10.13.161.34 15.20.58.14	El punto de origen es la dirección IP 209.85.221.45
From	Esta etiqueta presenta información de la cuenta que emite el correo electrónico, en este caso es:	La dirección de correo electrónico presente en esta etiqueta es	

	"kouadioyaoadamou17@gmail.com"	considerada como una dirección de correo electrónico de uso personal.	
To	La etiqueta mencionada presenta al receptor de la información del correo electrónico phishing.	Se aprecia que el atacante dirige el su acto a una sola persona con la siguiente dirección de correo electrónico: victoria.haz@hotmail.com	Se presume que el ataque fue solo a esa persona debido a que en la etiqueta TO no existe una lista de receptores del mensaje como aparece en el caso anterior.
ANALISIS DE CUERPO DE MENSAJE			
ETIQUETAS	**DESCRIPCIÓN**	**RESULTADOS**	**OBSERVACIÓN**
Content	En el correo electrónico presenta un supuesto comunicado de parte de una agencia gubernamental que busca que se cumpla una supuesta orden en contra de la propietaria del correo electrónico.	En el cuerpo del correo electrónico se tienen un mensaje corto y adjuntan un correo electrónico el cual el destinatario debe contactar: directionbpmcentre001@gmail.com	El correo electrónico a través del comunicado que adjunto tiene como objetivo hacer que la víctima ceda al miedo y contacte a la persona o al correo electrónico que se proporciona para comenzar con el engaño.

ANÁLISIS DE PÁGINA WEB			
NOMBRE DEL ARCHIVO	**DESCRIPCIÓN**	**RESULTADOS**	**OBSERVACIÓN**
Convocatoria	Supuesto informe de actos ilícitos cometidos por la persona que recibió el mensaje de correo electrónico.	Mediante el análisis por el algoritmo de VirusTotal se puede tener la seguridad de que el archivo no posee algún código malicioso insertado.	En el supuesto informe de parte del FBI, se puede notar el intento de edición, esto debido al uso de tipo de letras, colores y mala edición.

3.3.4 Caso 4 (Malware Troyano).

El archivo relacionado con el ejemplo a tratar en este punto es aquel denominado como "Fw RV su documento de flete y B_L.eml", el mismo que a través de técnicas de engaños motiva al receptor del correo electrónico a abrir el archivo adjunto en el mensaje.

Para acceder a la estructura del presente caso en el software AccessData se debe seleccionar el documento que posee la información que se requiere analizar. Toda la evidencia del análisis se lo puede encontrar en el Anexo 4.

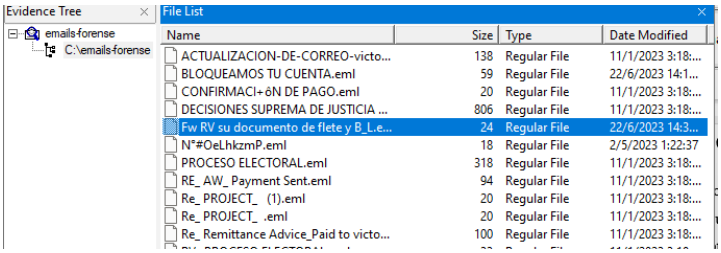


Fig.23. Información del archivo "Fw RV su documento de flete y B_L.eml"

Tabla VII: Análisis Caso 4

ANÁLISIS DE CABECERA			
(Ver Anexo 7)			
ETIQUETAS	**DESCRIPCIÓN**	**RESULTADOS**	**OBSERVACIÓN**
Received	La observación "Received" se repite 7 veces, eso representa a los diferentes saltos que el mensaje electrónico dio antes de llegar a la bandeja de entrada de la víctima.	Se aprecia que la cantidad de saltos en total son 7. Sin embargo, a través del análisis de pudo obtener 3 direcciones IP: 190.15.141.157 10.13.155.158 66.163.189.146	El punto de origen es la dirección IP 190.15.141.157
From	Esta etiqueta presenta información de la cuenta que emite el correo electrónico, en este caso es: saucinclubricantes@hotmail.com	La dirección de correo electrónico presente en esta etiqueta es considerada como una dirección de correo electrónico de uso personal.	
To	La etiqueta mencionada presenta al receptor de la información del correo electrónico malicioso.	Se aprecia que el atacante dirige el su acto a una sola persona con la siguiente dirección de	Se presume que el ataque fue solo a esa persona debido a que en la etiqueta TO no existe una lista de

		correo electrónico: victoria.haz@hotmail.com	receptores del mensaje como aparece en el caso anterior.
ANALISIS DE CUERPO DE MENSAJE			
ETIQUETAS	**DESCRIPCIÓN**	**RESULTADOS**	**OBSERVACIÓN**
Content	En el correo electrónico presenta un mensaje de parte de una agencia afirmando de que la generación de una factura había demorado.	En el cuerpo del correo electrónico se puede apreciar que adjunto en este tiene un archivo con extensión html.	El correo electrónico a través del comunicado que tiene como objetivo hacer que la víctima abra el documento y luego se infecte o ingresa a una página falsa.
ANÁLISIS DE PÁGINA WEB			
NOMBRE DEL ARCHIVO	**DESCRIPCIÓN**	**RESULTADOS**	**OBSERVACIÓN**
INV+BL+PL.pdf.html	Se presume que es una página web debido a su extensión html.	Mediante el análisis realizado por el algoritmo de VirusTotal, se verifica que el archivo adjunto en el correo electrónico posee virus de tipo troyano además de	La finalidad del archivo adjunto tiene como finalidad tratar de robar la información digital de una persona además de infectar su equipo informático.

		ser una página phishing.	

3.3.4 Caso 5 (Ingeniería social).

El archivo relacionado con el ejemplo a tratar en este punto es aquel denominado como "N°#OeLhkzmP.eml", el mismo que a través de técnicas de engaños motiva al receptor del correo electrónico a ceder a la promoción ofrecida por el remitente.

Para acceder a la estructura del presente caso en el software AccessData se debe seleccionar el documento que posee la información que se requiere analizar. Toda la evidencia del análisis se lo puede encontrar en el Anexo 4.

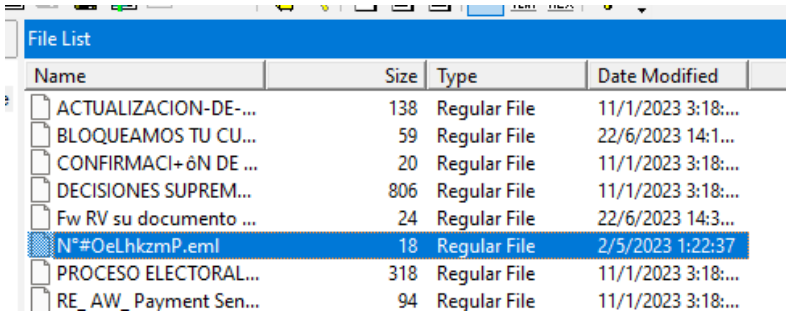


Fig.24. Información del archivo "N°#OeLhkzmP.eml"

Tabla VIII: Análisis Caso 5

ANÁLISIS DE CABECERA			
(Ver Anexo 8)			
ETIQUETAS	**DESCRIPCIÓN**	**RESULTADOS**	**OBSERVACIÓN**
Received	La observación "Received" se repite 5 veces, eso representa a los diferentes saltos que el mensaje electrónico dio antes de	Se aprecia que la cantidad de saltos en total son 5. Sin embargo, a través del análisis de	El punto de origen es la dirección IP 209.85.202.101

	llegar a la bandeja de entrada de la víctima.	pudo obtener 1 dirección IP: 209.85.202.101	
From	Esta etiqueta presenta información de la cuenta que emite el correo electrónico, en este caso es: renzonqc@gmail.com	La dirección de correo electrónico presente en esta etiqueta es de uso personal y del propietario de la cuenta que recibió el mensaje.	Es importante destacar que el correo electrónico es supuestamente enviado por la misma persona que lo recibe, la cabecera efectivamente aparece la dirección de correo electrónico del propietario aun cuando este asegura no haber hecho dicha acción.
To	La etiqueta mencionada presenta al receptor de la información del correo electrónico malicioso.	Se aprecia que el atacante dirige el su acto a una sola persona con la siguiente dirección de correo electrónico: renzonqc@gmail.com	El receptor es la misma persona que lo envía.
ANALISIS DE CUERPO DE MENSAJE			

ETIQUETAS	DESCRIPCIÓN	RESULTADOS	OBSERVACIÓN
Content	En el correo electrónico presenta un mensaje de ofertas que podría interesarle al receptor del mensaje de correo electrónico.	Mediante el análisis de esta parte se puede obtener que dentro del correo electrónico existen mensajes camuflados.	Los mensajes camuflados no los puede observar la persona propietaria del correo electrónico, sin embargo, estos también tratan de ofertas, suscripciones y demás movimientos electrónicos.

3.3.4 Caso 6 (Malware).

El archivo relacionado con el ejemplo a tratar en este punto es aquel denominado como "CONFIRMACI+ôN DE PAGO.eml", el mismo que a través de técnicas de engaños motiva al receptor del correo electrónico a ceder a la promoción ofrecida por el remitente.

Para acceder a la estructura del presente caso en el software AccessData se debe seleccionar el documento que posee la información que se requiere analizar. Toda la evidencia del análisis se lo puede encontrar en el Anexo 4.

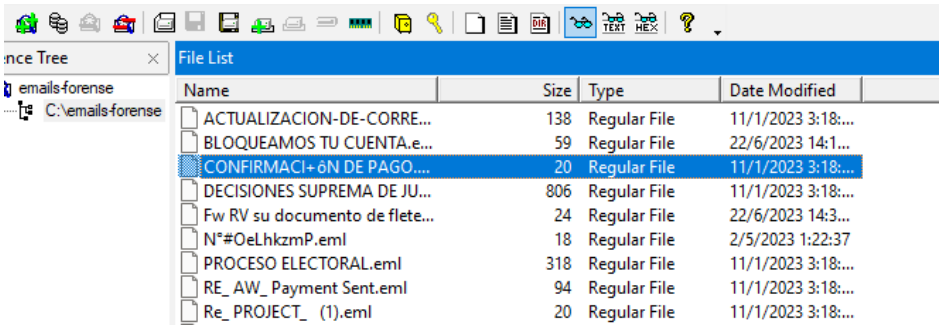


Fig.25. Información del archivo ""CONFIRMACI+ôN DE PAGO.eml"

Tabla IX: Análisis Caso 1

ANÁLISIS DE CABECERA			
(Ver Anexo 9)			
ETIQUETAS	**DESCRIPCIÓN**	**RESULTADOS**	**OBSERVACIÓN**
Received	La observación "Received" se repite 6 veces, eso representa a los diferentes saltos que el mensaje electrónico dio antes de llegar a la bandeja de entrada de la víctima.	Se aprecia que la cantidad de saltos en total son 6. Sin embargo, a través del análisis de pudo obtener 2 direcciones IP: 40.92.91.40 10.233.243.182	El punto de origen es la dirección IP 40.92.91.40
From	Esta etiqueta presenta información de la cuenta que emite el correo electrónico, en este caso es: sashasmith1001@hotmail.com	La dirección de correo electrónico presente en esta etiqueta es de uso personal.	
To	La etiqueta mencionada presenta al receptor de la información del correo electrónico malicioso.	Se aprecia que el atacante dirige el su acto a una sola persona con la siguiente dirección de correo electrónico: lidice_haz@hotmail.com	

ANALISIS DE CUERPO DE MENSAJE			
ETIQUETAS	**DESCRIPCIÓN**	**RESULTADOS**	**OBSERVACIÓN**
Content	En el correo electrónico presenta un mensaje de que se realizó una transferencia a su cuenta y que esta estará disponible en unos días	El atacante a través del uso de la ingeniería social busca que la victima abra el archivo adjunto.	Se encuentra adjunto un archivo que podría ser de interés para la víctima
ANÁLISIS DE ARCHIVO ADJUNTO			
ETIQUETAS	**DESCRIPCIÓN**	**RESULTADOS**	**OBSERVACIÓN**
Payment.html	Se presume que es una página web debido a su extensión html.	Mediante el análisis realizado por el algoritmo de VirusTotal, se verifica que el archivo adjunto en el correo electrónico es peligroso.	El archivo para este caso no presenta ningún tipo de Malware o phishing según la herramienta antes mencionada.

3.2.4. DOCUMENTACIÓN

En esta fase se emite un informe de opiniones y conclusiones sobre las evidencias obtenidas por cada uno de los casos analizados; la información relacionada con este apartado se puede encontrar en el Anexo 10 (Ver Anexo 10).

CAPITULO IV RESULTADOS

4.1. INTERPRETACIÓN DE LA INFORMACIÓN

4.1.1. Cuadros y gráficos estadísticos de encuestas

La encuesta utilizada se encuentra en el anexo 4, esta fue dirigida al personal educativo de la institución; y su objetivo fue identificar el nivel de uso de los correos electrónicos, así mismo como identificar el porcentaje estimado de víctimas de ciberataques dentro de ese contexto.

Pregunta 1 Frecuencia de uso de correo electrónico

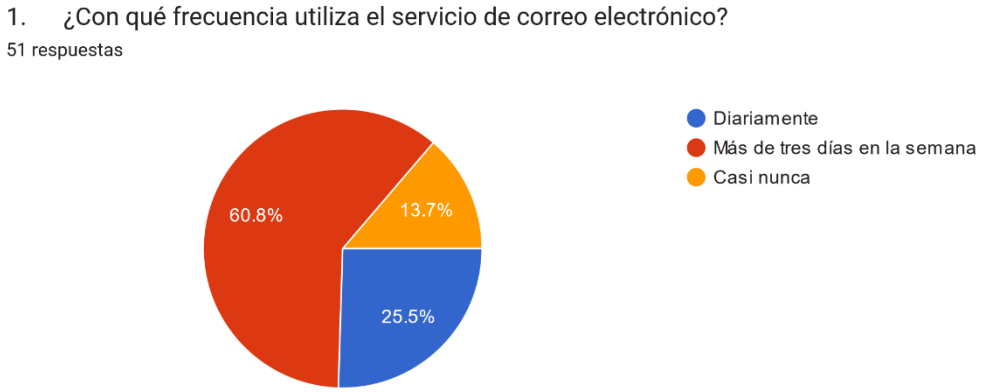


Fig.26. Frecuencia de uso de correo electrónico

El 60.8% de los encuestados contestó que utilizan el correo electrónico más de 3 veces en la semana, sin embargo, alrededor del 13.7% de las personas aseguran que no usan el servicio con frecuencia.

El nivel de frecuencia puede exponer al usuario en un riesgo más alto con respecto a la materialización de un ciberataque por medio de la mensajería electrónica.

Es necesario incentivar al uso de las herramientas digitales, así mismo como las medidas de seguridad necesarias para una correcto uso y desempeño de estas.

PREGUNTA 2 Servicio electrónico con mayor uso

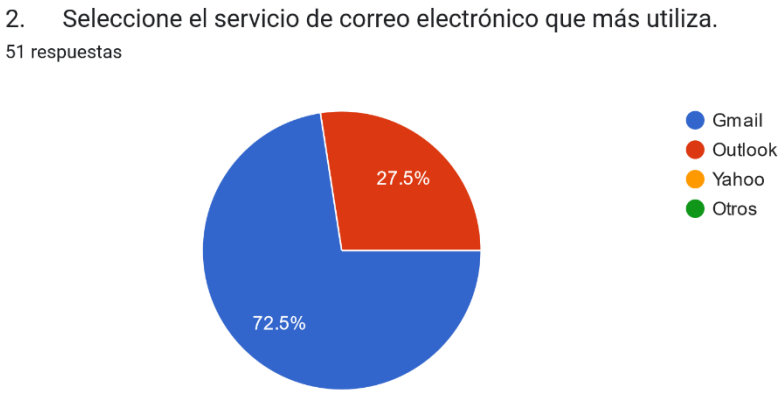


Fig.27. Servicio electrónico con mayor uso

Según la encuesta realizada el 72,5% de las personas usan Gmail como plataforma preferida de correo electrónico, seguida por Outlook con el 27.5%.

El propósito es conocer las plataformas más usadas de correo electrónico y el uso que estos usuarios le dan mediante las herramientas integradas en estas.

Es de utilidad conocer las plataformas porque de esa manera se puede recomendar un conjunto de buenas prácticas basadas en el entorno que manejan estas mismas.

PREGUNTA 3 Ciberataques de correos electrónicos

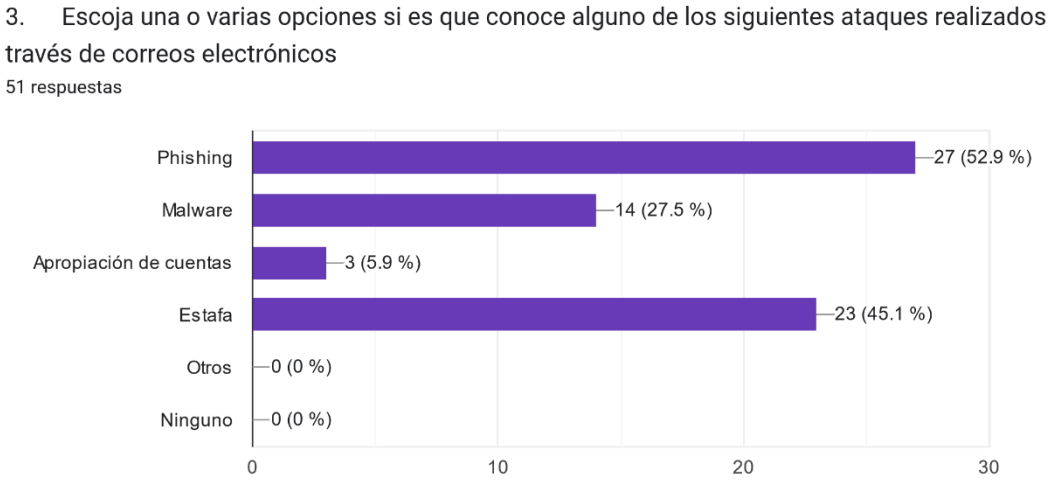


Fig. 28. Ciberataques de correos electrónicos

Según la encuesta del listado proporcionado de ciberataques entre 23 y 27 personas aseguran que conocen lo que es el phishing y las estafas a través de correos electrónicos, por otra parte, la apropiación de cuentas no es tan conocida por los usuarios debido a que solo 3 personas tienen de toda la población tiene conocimiento sobre aquello.

Mediante esta pregunta se puede medir el conocimiento de los individuos sobre las amenazas a las que se exponen cuando usan el servicio de correo electrónico. El desconocimiento de la mayoría de las personas sobre los ataques es evidente por lo son más propensas a ser víctimas de estos.

Es necesario poseer conocimiento sobre estos ciberataques y su operatividad para así asumir un método de prevención.

PREGUNTA 4 Nivel de conciencia sobre los delitos electrónicos

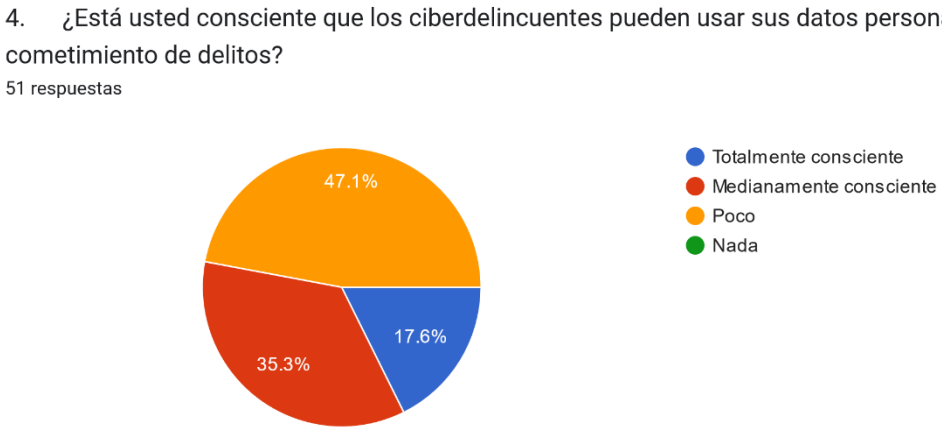


Fig.29. Nivel de conciencia sobre los delitos electrónicos

El 47.1% de la población se encuentra poco consciente de que la información que se proporciona a través de medios digitales puede ser objetivo de robo por ciberdelincuentes para actos ilícitos, su contraparte que pertenece al 17.6% si tiene conocimiento sobre aquellas actividades

La finalidad es conocer el nivel de conciencia sobre las actividades que los ciberdelincuentes pueden realizar con la información personal que está colgada en la red.

Es necesario incentivar al cuidado de la información digital ya que toda persona que tenga su información visible dentro de la web es propensa a sufrir este tipo de ataques contra ellos o en contra de otras personas usando su identidad.

PREGUNTA 5 Víctimas de ciberdelitos

Fig.30. Víctimas de ciberdelitos

Según la encuesta el 76.5% de las personas encuestadas fueron víctimas de algún tipo de ciberataque, por otra parte, el resto conformado por el 23.5% no ha sido víctima de los ciberdelincuentes.

El propósito es tener conocimiento sobre la interacción que ciertas personas de la población tuvieron con ciberataques a través de correos electrónicos.

Es necesario incluir la ciberseguridad de datos personales cuando se usan herramientas como el correo electrónico.

PREGUNTA 6 Tipo de delito

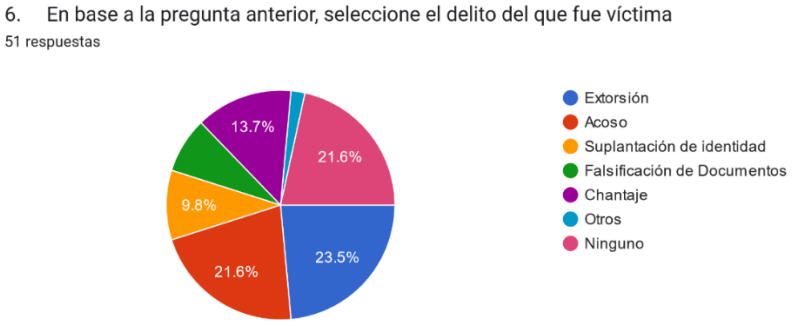


Fig.31. Tipo de delito

El 21.6% no fue víctima de ninguno de los ataques expuestos en la encuesta, por otra parte, el resto está distribuido en diferentes delitos como el chantaje perteneciente al 13.7%.

El propósito es conocer el tipo de ataque con el que los individuos tuvieron la interacción para después emitir consejos para evitar caer en aquellos.

Es necesario tener conocimiento sobre los tipos de ciberataques y sus distintos métodos de prevención.

PREGUNTA 7 Métodos de seguridad

Fig.32. Métodos de seguridad

Según la encuesta el 80.4% de la población considerada usa el antivirus como método de seguridad frente a los ciberataques, por otra parte, el resto representado por el 19.6% está dividido en las diferentes herramientas.

La finalidad es conocer los métodos de defensa que posee la población en el caso de presentarse un incidente de seguridad y que tan factible o confiable es la herramienta utilizada.

Es necesario integrar el uso de herramientas de protección de datos personales para preservar y garantizar la disponibilidad de estos mismos.

PREGUNTA 8 Medios de información

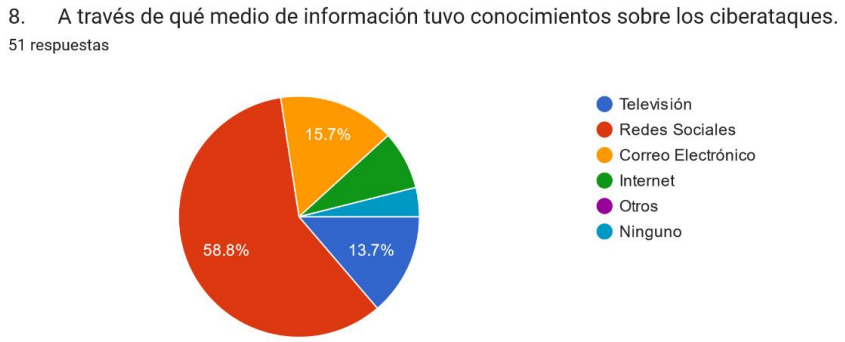


Fig.33. Medios de información

El 58.6% de la población tiene conocimiento sobre los ciberataques gracias a las redes sociales y con una representación del 3.9% se obtiene que ese porcentaje no tiene conocimiento sobre aquello.

La finalidad es evaluar el conocimiento de las personas relacionado con los ciberataques y sobre los métodos de información que permiten conocer este tipo de actos delictivos. El conocer de la existencia de un ciberataque no significa que pueden defenderse o prevenir este mismo.

La información y conocimientos es esencial por lo que es necesario tomar conciencia de los riesgos latentes en un servicio de correo electrónico.

PREGUNTA 9 Configuración de gestión de correos electrónicos

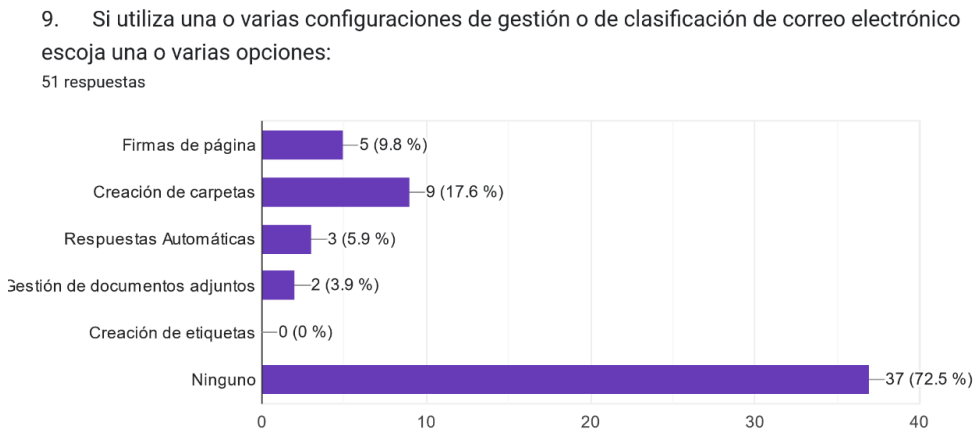


Fig.34. Configuración de gestión de correos electrónicos

El 72.5% que es representado por 37 personas afirman que no usan métodos de gestión o clasificación de un correo electrónico además que el 3.9% representado por 2 personas utilizan la gestión de documentos adjuntos.

La finalidad es saber el grado de uso que le dan a la mensajería electrónica ya que posee diferentes herramientas de organización, respuesta, carpetas entre otras.

Es fundamental incluir el uso de diferentes herramientas de gestión de correos electrónicos, esto da la posibilidad de tener organizado los diferentes pendientes del trabajo o asuntos personales.

PREGUNTA 10 Verificación de emisor en el correo electrónico

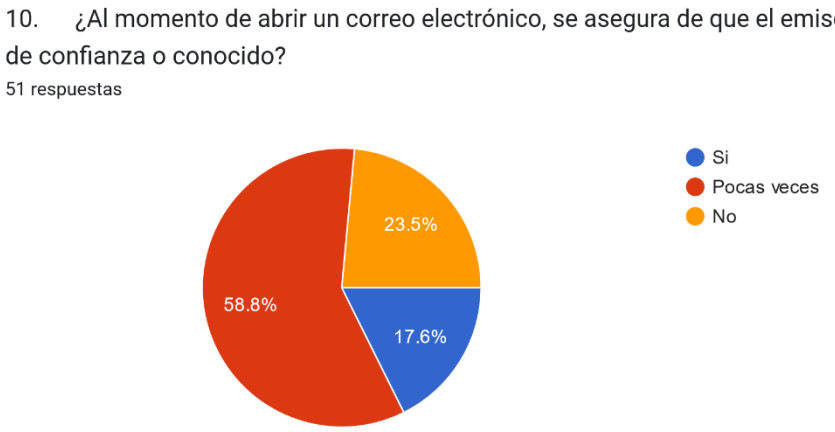


Fig.35. Verificación de emisor en el correo electrónico

El 58.8% de la población aseguro que visualiza pocas veces el emisor del correo electrónico, por otra parte, el 17.6% si revisa el remitente de los correos electrónicos presentes en su bandeja de entrada.

El visualizar el emisor del mensaje es parte fundamental para evitar caer en algún acto delictivo, actividad que la población considerada no realiza.

Adicional a las encuestas se realizó una prueba de laboratorio, esta misma consistía en mostrar un correo electrónico y los individuos tenían que tratar de identificar si era un correo electrónico auténtico o era un correo electrónico fraudulento, los correos

electrónicos fueron los mismos usados en la presente investigación y otros sacados de internet para realizar la práctica.

Dando como resultado que 5 personas representando el 9,8% de la población pudo identificar correctamente la amenaza, sin embargo, el resto de las personas no sabía cómo estos se identificaban o reconocían. Por lo que se concluye y se afirma la hipótesis tratada en este apartado de que a mayor ataque de correos electrónicos mayor número de personas afectadas.

4.2 INTERPRETACIÓN DE RESULTADOS EXPERIMENTALES

4.2.1 Evaluación de las características de integridad de un correo electrónico

A continuación, se describen 5 propiedades necesarias que permitan identificar la integridad de un correo electrónico. En este proyecto se han considerado la veracidad de la fuente, autenticidad el contenido, detalles del contacto, lenguaje y gramática, solicitudes inusuales. Debajo de cada característica se define los valores a evaluar especificando la puntuación considerada para cada ejemplo.

Veracidad de la fuente. – Tener en consideración si el correo electrónico proviene de una fuente confiable como una empresa además de que el dominio coincida con el nombre de la institución que se identifica.

Etiquetas de evaluación: From, Thread Topic (Ver Anexo 3)

- Si el remitente es una fuente conocida y confiable. Puntuación = 0
- Si el remitente es sospechoso. Puntuación = 1

Autenticidad del contenido. – Evaluar si el contenido es auténtico o existe algún tipo de manipulación de parte del remitente.

Detalles a evaluar: Archivos adjuntos

- Si el contenido no es manipulado y confiable. Puntación = 0
- Si el contenido es manipulado. Puntuación = 1

Detalles del contacto. – Verificar si el correo electrónico posee información de contacto válida y legítima.

Etiquetas a evaluar: From, Thread Topic que se encuentran en la cabecera del correo electrónico (Ver Anexo 3).

- Si existe información completa y verificable del contacto. Puntación = 0
- Si no se proporciona información de contacto o es sospechosa. Puntuación = 1

Lenguaje y gramática. – Considerar la manera de utilizar la gramática y el uso del lenguaje escrito en el correo electrónico.

Detalles a evaluar: Archivos adjuntos y contenido del mensaje electrónico

- Si el texto es coherente y bien escrito. Puntuación = 0
- Si el texto contiene errores o no es coherente. Puntuación = 1

Solicitudes inusuales. – Identificar si el correo electrónico posee solicitudes inusuales como solicitud de información personal o financiera.

Detalles a evaluar: Contenido del mensaje electrónico y links proporcionados

- Si no hay solicitudes inusuales. Puntación = 0
- Si hay solicitudes inusuales de información. Puntuación = 1

La siguiente tabla presenta el formato de evaluación o clasificación de las características a evaluar para cada uno de los casos.

Tabla X: Modelo de evaluación de riesgo

Riesgo Bajo	
Riesgo Medio	
Riesgo Alto	

		Nivel de riesgo				
Características	Veracidad de la fuente					
	Autenticidad del contenido					

	Detalles del contacto					
	Lenguaje y gramática					
	Solicitudes inusales					
		Veracidad de la fuente	Autenticidad del contenido	Detalles del contacto	Lenguaje y gramática	Solicitudes inusales

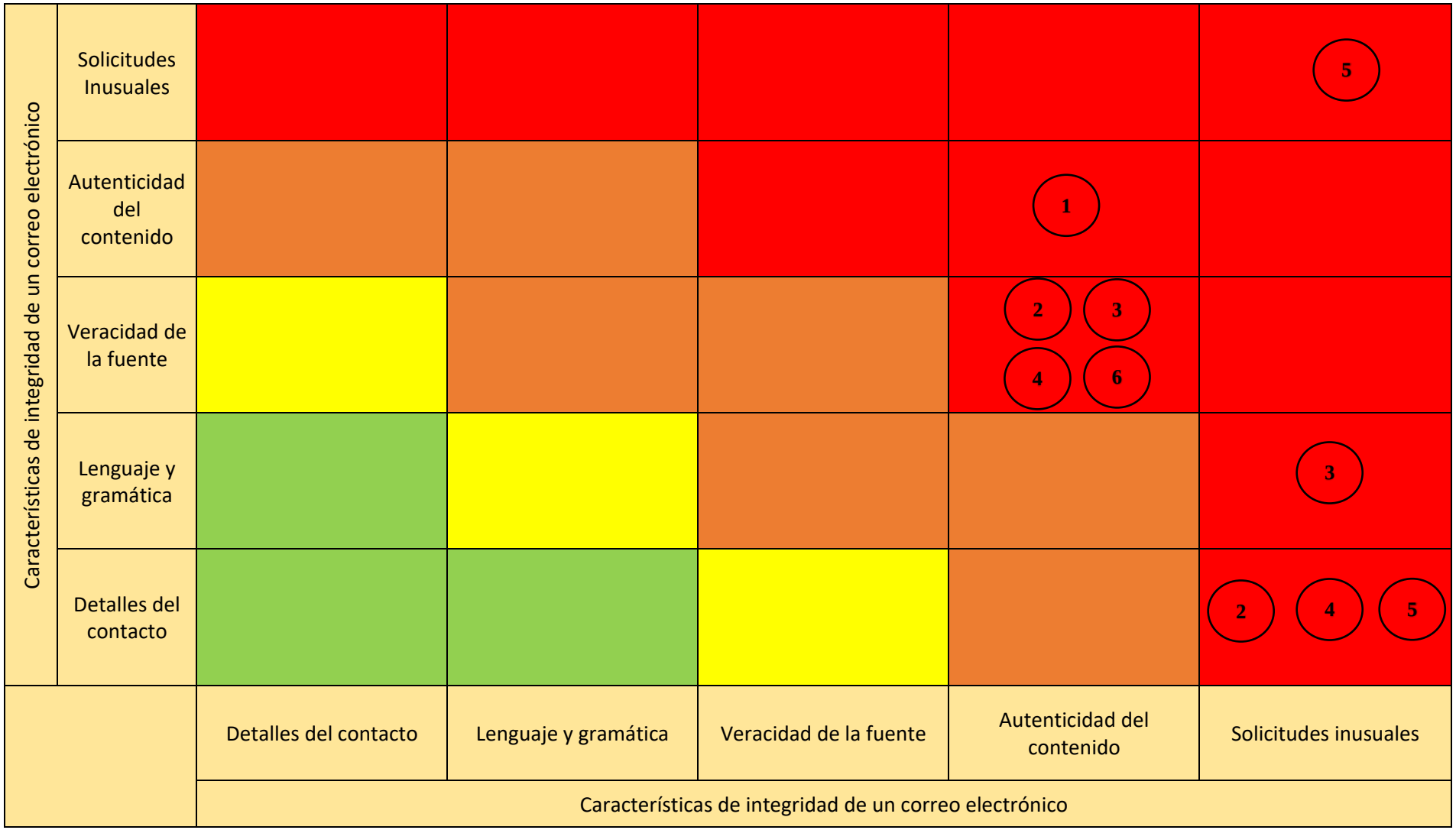
A continuación, se realiza la evaluación manual de las características mencionadas con anterioridad en donde se considera que el valor de 0 es un indicador positivo que el correo electrónico puede ser de confianza, por otra parte, el valor 1 representa que se está levantando sospechas, esto debido a que no se está considerando como un mensaje de correo electrónico confiable.

Tabla XI: Evaluación manual de características

N° de Caso	**Tipo de correo electrónico**	**Evaluación de características de integridad de correos electrónicos**					**Total**
		Veracidad de la fuente	**Autenticidad del contenido**	**Detalles del contacto**	**Lenguaje y gramática**	**Solicitudes inusuales**	
Caso 1	Correo electrónico zombie	0	1	0	0	1	2
Caso 2	Correo electrónico Phishing	1	1	1	0	1	4

Caso 3	Correo electrónico fraudulento o engañoso	1	1	0	1	1	4
Caso 4	Correo electrónico con Malware Troyano	1	1	1	0	1	4
Caso 5	Correo electrónico con Ingeniería Social	0	1	1	0	1	3
Caso 6	Correo electrónico con Malware	1	1	0	0	1	3

Tabla XII: Categorización del nivel de riesgo



4.3. ESTÁNDARES PARA GESTIONAR LA SEGURIDAD DEL SERVICIO DE CORREO ELECTRÓNICO.

A continuación, se presenta una comparación entre el estándar ISO y NIST, tomando en cuenta las siguientes características a evaluar: Descripción, aplicación, número de fases de implementación, fases y ventajas.

Tabla XIII: Estándares ISO 27000 Y NIST

	Estándares	
	ISO 27000	NIST
DESCRIPCIÓN	ISO es considerada como una red que la conforman diferentes organismos internaciones de estandarización con alrededor de 160 países, es así que ISO propone la utilización de un SGSI que sirve para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección de los activos de información empresariales.	Es una agencia no reguladora del Departamento de Comercio de los Estados Unidos. Esta institución posee un marco de seguridad, la misma que es considerada como una guía que se basa en estándares internacionales, pautas y buenas prácticas ya existentes para que se puedan implementar en las organizaciones y así administrar y reducir el riesgo en el ámbito informático y tecnológico.
APLICACIÓN	Implementa un conjunto de buenas prácticas implantadas en el Sistema de Gestión de Seguridad de	Para la implementación de este marco de seguridad es esencial seguir un proceso continuo de identificación,

	la Información. Cumpliendo con un régimen de legalidad para preservar su identidad, integridad y la confidencialidad de la información que emplean.	evaluación y accionar frente al riesgo. El uso de este estándar ofrece la capacidad de cuantificar y comunicar los cambios a los programas de ciberseguridad ya existentes en ámbito.
N° FASES DE IMPLEMENTACIÓN	4 fases	5 fases
FASES	Diagnostico Planificación Implementación Evaluación	Identificar Proteger Detectar Responder Recuperar
VENTAJAS	Permite que los procesos de seguridad estén equilibrados y a la vez coordinados entre sí. Posibilita la activación de alertas en caso de que se llegue a presentar alguna actividad sospechosa. Permite hacerles seguimiento a los controles	Determinar prioridades y alcance mediante los objetivos que posee una empresa. Identifica los sistemas y activos relacionas con el alcance del programa y sus políticas. Analizar el entorno y el estado de los activos para determinar si existe una vulnerabilidad a explotar.

	de seguridad. Genera valor agregado para la compañía, pues aún no son muchas las empresas que cuentan con la certificación de seguridad en la información.	

4.4 BUENAS PRÁCTICAS PARA USAR Y ADMINISTRAR LA SEGURIDAD INFORMÁTICA DEL SERVICIO DE CORREO ELECTRÓNICO

A continuación, se presenta un conjunto de buenas prácticas para administrar eficientemente el uso del correo electrónico.

- Analizar la cabecera y verificar que la dirección de correo electrónico de una institución no se encuentre asociada a una cuenta de correo electrónico personal.
- La verificación de la dirección de correo electrónico recibido es importante debido a que contiene información y poseen características que permiten reconocer un posible ataque de phishing.
- Capacitarse o informarse para evitar caer en un ataque de phishing, la mayoría de los bancos del país emiten comunicados en donde exponen tips sobre como identificar y reconocer un ataque de phishing.
- Si por algún motivo ingresa a un enlace adjunto, el navegador lanzará un mensaje de advertencia de que el sitio puede ser peligroso debido a que en este enlace no posee el protocolo de seguridad conocido como https. Si aún decide ingresar al sitio web es importante que no coloque ningún tipo de información real que pueda comprometer: correo electrónico, cuentas bancarias, datos personales, redes sociales y localidad.

- Analizar el contenido debido a que estos correos electrónicos fraudulentos se caracterizan por poseer un mensaje que sea de importancia para la víctima aplicando técnicas de ingeniería social.
- Si el correo electrónico posee enlaces adjuntos es recomendable analizarlo en una plataforma web (Virus Total) o una que sea de confianza, ya que esta brindará información acerca del sitio web. En el mejor de los casos la dirección web no está disponible y en el peor, es el enlace para descargar un software malicioso en la PC, eh aquí la importancia del análisis de enlaces.
- Leer detenidamente el cuerpo del correo electrónico para identificar un intento ataque a través de la mensajería electrónica.
- Si el tipo de correo electrónico posee algún enlace adjunto es necesario evaluar la confiabilidad de este mismo.
- Analizar el archivo con un antivirus si se da el caso de que se llega a descargar, si a través de la visualización presenta sospechas de un posible ataque lo mejor es no descargar el archivo adjunto.
- Analizar enlaces, imágenes y documentación adjunta. Si presenta sospechas desde el análisis del mensaje lo recomendable es ignorar lo demás.
- Observar detenidamente el emisor del mensaje ya que puede tratarse de un ataque de phishing en donde utilicen ingeniería social para hacer descargar un documento o entra el enlace a la víctima

Conclusiones

El 76.5% de los encuestados mencionaron ser víctimas de ciberataques a través del servicio de correo electrónico. Esto se evidencia debido a su falta de información sobre los métodos de protección frente a este tipo de ataques.

Mediante el uso de herramientas de código abierto, se puede realizar una investigación forense permitiendo así obtener direcciones IP, Mac, direcciones de correo electrónico, y demás identificadores digitales que permitan llegar al posible ciberdelincuente responsable de los ataques.

En la comparación de estándares internacionales se puede obtener puntos importantes como el método de implementación y las fases que constan en cada una de estas, lo cual es información valiosa para una empresa que quiere regirse a una normativa internacional, sin embargo, las buenas prácticas emitidas en este trabajo fueron dirigidas hacia el personal educativo de una institución para que estos tengan conocimiento sobre el actuar al presentarse los ciberataques.

La cabecera de un correo electrónico presenta alrededor de 13 etiquetas, de las cuales destacan 3; Received, From y Thread-Index. Se considera a las etiquetas anteriores como las más importantes en un análisis informático forense debido a la información que presentan; dirección IP, número de saltos, fecha y hora de envió y características que sirven para encontrar al ciberdelincuente.

Considero que la mejor herramienta para el análisis informático forense en correos electrónicos es Message Header Analyzer, debido a que su algoritmo permite observar la información requerida en el análisis de manera rápida y ordenada, en comparación a otras herramientas que se utilizan para este tipo de actividades.

Recomendaciones

Es necesario que, los usuarios se mantengan más informados respecto a los nuevos ciberataques, no solo enfocados en correos electrónicos, sino en los diferentes ciberamenazas que se pueden llegar a materializar en los espacios virtuales, y poner en riesgos los datos personales.

Para el análisis digital forense, es necesario implementar y configurar un ambiente virtual aislado que permita realizar las pruebas y experimentación de los correos maliciosos, y con ello evitar infecciones o proliferación de malware.

El uso y la implementación de estándares internacionales es esencial para avalar la seguridad de la información de una empresa o institución, en caso de que se presente un incidente, ataque o evento de ciberseguridad; por lo que, se requiere implementar frameworks de trabajo y de buenas prácticas que ayuden a que el flujo de información sea seguro y eficaz.

Bibliografía

[1] "Vista de Sistema Multi-agente para la Detección de Fraudes en el Correo Electrónico." http://difu100cia.uaz.edu.mx/index.php/difuciencia/article/view/87/55 (accessed Nov. 15, 2022).

[2] C. L. Paredes Vargas and E. en A. Gerencia, "OPORTUNIDADES DE MEJORA DETRÁS DE LA PRINCIPAL PREOCUPACIÓN DEL SISTEMA FINANCIERO: FRAUDES INFORMÁTICOS," Especialización en Alta Gerencia, Jul. 2021.

[3] A. Trejo, B. Pihuave, and C. Cisneros, "Application of forensic science in cybercrime in Ecuador and its punishability | Aplicación de la ciencia forense en los delitos informáticos en el Ecuador y su punibilidad," *Espacios*, vol. 39, no. 42, 2018.

[4] ESET, "Security Report LATAM 2017," pp. 1–21, 2017.

[5] J. W. C. Mirabal, "ACOSO Y FRAUDE CIBERNETICO ANALISIS DEL CASO: USA V. STEVEN WAITHE," EDP UNIVERSITY, 2022.

[6] A. El, P. D. E. Las, D. Mabel, B. Arroyave, A. Beatriz, and E. Henao, "Facultad de Ciencias Administrativas y Económicas. Tecnológico de Antioquia Institución Universitaria Trabajo de Grado. Ciclos Profesionales," 2017.

[7] "Análisis forense informático de un servidor de archivos institucional." https://repositorio.pucesa.edu.ec/handle/123456789/3480 (accessed Nov. 16, 2022).

[8] "Análisis Forense – CVS." https://cvs.ec/2020/07/16/analisis-forense/ (accessed Feb. 21, 2023).

[9] "Modelo SKRAM - DragonJAR." https://www.dragonjar.org/modelo-skram.xhtml (accessed Feb. 21, 2023).

[10] "Informática forense: Qué es, como realizar un análisis forense." https://protecciondatos-lopd.com/empresas/informatica-forense/#Objetivos_del_computo_forense (accessed Feb. 21, 2023).

[11] “5 fases fundamentales del análisis forense digital | WeLiveSecurity.” https://www.welivesecurity.com/la-es/2015/04/15/5-fases-analisis-forense-digital/ (accessed Jan. 15, 2023).

[12] I. M. H. Cajo, S. Y. Pucuna, B. G. H. Cajo, V. M. O. Coronado, and F. V. S. Orozco, “Estudio Comparativo De Las Metodologías De Análisis Forense Informático Para La Examinación De Datos En Medios Digitales,” *Eur. Sci. Journal, ESJ*, vol. 14, no. 18, p. 40, 2018, doi: 10.19044/esj.2018.v14n18p40.

[13] “CAINE Live USB/DVD - análisis forense informático análisis forense digital.” https://www.caine-live.net/ (accessed Nov. 22, 2022).

[14] “QFileHasher download | SourceForge.net.” https://sourceforge.net/projects/qfilehasher/ (accessed Nov. 22, 2022).

[15] “Visor de Metadatos.” https://www.extractmetadata.com/es.html (accessed Nov. 22, 2022).

[16] “FTK Imager - Exterro.” https://www.exterro.com/ftk-imager (accessed Feb. 21, 2023).

[17] “Qué es VirusTotal |.” https://www.innovaciondigital360.com/cyber-security/que-es-virustotal/ (accessed Jul. 18, 2023).

[18] “Message Header Analyzer - Connectivity Analyzer | Microsoft Learn.” https://learn.microsoft.com/en-us/connectivity-analyzer/message-header-analyzer (accessed Jul. 23, 2023).

[19] V. Huamani, “Uso de plataformas web informativas para el fortalecimiento de la comunicación en los espacios universitarios,” *Front. en ciencias Soc. y humanidades*, vol. 2, no. 1, pp. 269–279, Mar. 2023.

[20] “Informe de spam y phishing, tercer trimestre de 2021 | Securelist.” https://securelist.lat/spam-and-phishing-in-q3-2021/95710/ (accessed Apr. 12, 2023).

[21] “Número de archivos maliciosos detectados cada día alcanzó 380 mil en 2021 | Blog oficial de Kaspersky.” https://latam.kaspersky.com/blog/numero-de-archivos-maliciosos-detectados-cada-dia-alcanzo-380-mil-en-2021/23689/

(accessed Jul. 23, 2023).

[22] E. Secretaria Nacional de Planificacion, “Plan-de-Creación-de-Oportunidades-2021-2025-Aprobado,” *Plan de Creación de Oportunidades 2021-2025*. pp. 43-48-85–90, 2021. [Online]. Available: file:///C:/Users/PC-CARO/Documents/Plan-de-Creación-de-Oportunidades-2021-2025-Aprobado.pdf%0Ahttps://observatorioplanificacion.cepal.org/es/planes/plan-nacional-de-desarrollo-2017-2021-toda-una-vida-de-ecuador

[23] N. Morales, “Investigación Exploratoria : Tipos , Metodología y Ejemplos”.

[24] A. Valle, *La Investigación Descriptiva con Enfoque Cualitativo en Educación*. 2022. [Online]. Available: https://files.pucp.education/facultad/educacion/wp-content/uploads/2022/04/28145648/GUIA-INVESTIGACION-DESCRIPTIVA-20221.pdf

[25] “Investigación empírica » Técnicas de Investigación.” https://tecnicasdeinvestigacion.com/investigacion-empirica/ (accessed Jun. 28, 2023).

[26] “¿Qué es la seguridad del correo electrónico? | Cloudflare.” https://www.cloudflare.com/es-es/learning/email-security/what-is-email-security/ (accessed Jan. 18, 2023).

[27] B. Networks, W. Blvd, B. Networks, B. Networks, B. Networks, and E. Unidos, “Trece tipos de amenazas de correo electrónico que debe conocer Índice,” vol. 4772, 2020.

[28] A. R. GARCIA MONGE, “Seguridad Informáticay el Malware,” pp. 1–11, 2017, [Online]. Available: http://repository.unipiloto.edu.co/handle/20.500.12277/2641

[29] T. D. E. Grado, “Confiabilidad de las herramientas informáticas forense,” p. 12, 2011.

[30] C. A. Puerta and A. S. Upegui, “El correo electrónico: herramienta que favorece la interacción en ambientes educativos virtuales The Electronic Mail: A Tool that Benefits the Interaction in Educational Virtual Environments Le courrier éle,” *Tipo artículo Result. Investig. científica y tecnológica 1* ., p. 28, 2010, [Online]. Available: https://www.redalyc.org/pdf/1942/194214476003.pdf

[31] “Análisis Forense Informático - Ciberseguridad.” https://www.grupoacms.com/analisis-forense-informatico-ciberseguridad (accessed Apr. 27, 2023).

[32] “Informática Forense: El Modelo SKRAM | by Marvin G. Soto | Medium.” https://marvin-soto.medium.com/informática-forense-el-modelo-skram-19c9600cced7 (accessed May 23, 2023).

[33] M. B. A. I. H. B. P, “Pericias en correos electrónicos”.

[34] J. Andrés, O. Castro, L. Gisell, and B. Montilla, “Análisis Forense a correos electrónicos en Outlook”, [Online]. Available: www.microsoft.com/en-us/outlook-com

[35] “Estándar internacional _ AcademiaLab.” https://academia-lab.com/enciclopedia/estandar-internacional/ (accessed Apr. 27, 2023).

[36] M. F. Delgado, “Taller de Implementación de la norma ISO 27001,” *Of. Nac. Gob. Electrónico e Informática*, 2017, [Online]. Available: www.pecert.gob.pe/images/publicaciones/4.pdf

[37] “EvaluacionRiesgo.png (Imagen PNG, 1226 × 1024 píxeles) - Escalado (54 %).” https://www.normas-iso.com/wp-content/uploads/2012/02/EvaluacionRiesgo.png (accessed Jan. 25, 2023).

[38] NQA, “Iso 27001:2013 Guía De Implantación Para La Seguridad De La Información,” *Nqa*, vol. 1, pp. 1–30, 2017, [Online]. Available: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

[39] “Análisis y evaluación de riesgos en ISO 27001.” https://www.pmg-ssi.com/2019/06/analisis-y-evaluacion-de-riesgos-en-iso-27001-amenazas-consecuencias-y-criticidad/ (accessed Jan. 25, 2023).

[40] “Ciclo-de-PDCA-1024x522.jpg (Imagen JPEG, 1024 × 522 píxeles).” https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/08/Ciclo-de-PDCA-1024x522.jpg (accessed Jan. 25, 2023).

[41] “¿Qué es NIST Cibersecurity Framework? | GSS.”

https://www.globalsuitesolutions.com/es/que-es-nist-cibersecurity-framework/ (accessed Jun. 27, 2023).

[42] "¿Qué es el marco de ciberseguridad del NIST? | IBM." https://www.ibm.com/mx-es/topics/nist (accessed Jun. 27, 2023).

[43] OEA, "Ciberseguridad: Marco Nist," *White Pap. Ser.*, p. 20, 2019, [Online]. Available: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

[44] J. M. Amy Mahn, "Primeros pasos de NIST Marco de ciberseguridad," *Prim. pasos NIST*, vol. 1, 2021, [Online]. Available: https://www.google.com/search?q=nist&rlz=1C1VDKB_esEC996EC996&oq=nist&aqs=chrome.0.69i59j69i57j35i39i362l5j69i60.438j0j7&sourceid=chrome&ie=UTF-8

[45] "Marco de ciberseguridad del NIST | Comisión Federal de Comercio." https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist (accessed Jun. 28, 2023).

[46] "¿Qué es el correo electrónico? | Definición de correo electrónico | Cloudflare." https://www.cloudflare.com/es-es/learning/email-security/what-is-email/ (accessed Apr. 27, 2023).

[47] "Phishing: ¿qué es y como evitarlo? - Panda Security." https://www.pandasecurity.com/es/security-info/phishing/ (accessed Apr. 28, 2023).

[48] "Evitar la apropiación de cuentas | Microsoft Dynamics 365." https://dynamics.microsoft.com/es-es/ai/fraud-protection/account-takeover/ (accessed May 17, 2023).

[49] "Peritaje de correos electrónicos - Indalics." https://indalics.com/servicios-periciales/peritaje-de-correos-electronicos (accessed May 17, 2023).

[50] "Protocolos TCP/IP - Documentación de IBM." https://www.ibm.com/docs/es/aix/7.1?topic=protocol-tcpip-protocols (accessed Jul. 05, 2023).

[51] “Protocolos de seguridad informática para empresas | Grupo Atico34.” https://protecciondatos-lopd.com/empresas/protocolos-seguridad-informatica/#Que_son_los_protocolos_de_seguridad_informatica (accessed Jul. 05, 2023).

[52] “¿Qué es el POP3? - Dommia.” https://www.dommia.com/es/faqs/que-es-el-pop3 (accessed Jul. 05, 2023).

[53] “¿Qué es acceso al correo mediante IMAP?” https://www.hostinet.com/formacion/correo-electronico/que-es-acceso-correo-mediante-imap/ (accessed Jul. 05, 2023).

[54] “¿Qué son IMAP y POP? - Soporte técnico de Microsoft.” https://support.microsoft.com/es-es/office/-qué-son-imap-y-pop-ca2c5799-49f9-4079-aefe-ddca85d5b1c9 (accessed Jul. 05, 2023).

[55] “Protocolo simple de transferencia de correo (SMTP) - Documentación de IBM.” https://www.ibm.com/docs/es/i/7.3?topic=information-smtp (accessed Jul. 06, 2023).

[56] “¿Qué es el protocolo simple de transferencia de correo (SMTP)? | Cloudflare.” https://www.cloudflare.com/es-es/learning/email-security/what-is-smtp/ (accessed Jul. 06, 2023).

[57] “My Email Communications Security Assessment (MECSA).” https://mecsa.jrc.ec.europa.eu/es/about (accessed Jul. 23, 2023).

[58] “Seguridad Informatica.” https://www.uacj.mx/CGTI/CDTE/JPM/Documents/IIT/infseguridad/U2-5.html (accessed Jul. 23, 2023).

[59] “Qué es email spoofing: suplantación de identidad en correos electrónicos.” https://www.welivesecurity.com/la-es/2021/03/23/que-es-email-spoofing-suplantacion-identidad-correos-electronicos/ (accessed Jul. 23, 2023).

[60] “Seguridad del correo electrónico - Documentación de IBM.” https://www.ibm.com/docs/es/i/7.3?topic=options-e-mail-security (accessed Jul. 23, 2023).

[61] F. G. Kaiser and M. Wilson, *código orgánico integral penal RO.pdf*, vol. 30, no. 5. 2000. [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1111/j.1559-1816.2000.tb02505.x/abstract%5Cnchrome://zotero/content/tab.xul

[62] Asamblea Nacional de la República del Ecuador, "Ley Organica De Proteccion De Datos Personales," pp. 1–70, 2021.

[63] C. Nacional, L. E. Y. D. E. C. Electronico, E. Y. M. D. E. Datos, T. Preliminar, and P. Generales, "Ley de comercio electronico, firmas y mensajes de datos," pp. 1–17, 2002, [Online]. Available: https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf?fbclid=IwAR2PhfFJMvEU4S0R_nYNE2--YV9mjaGvZ-eTb0efkBpKn5QEgmnrIwJeGMA

Anexos

Anexo 1

REVISTA ESPACIOS

Según la revista espacios los ataques informáticos son más comunes de los normal, sin embargo, las personas no se atreven a denunciar por diversas razones. Es así como se obtiene un porcentaje estimado de los fraudes informáticos que han realizado en el Ecuador, por este motivo los peritos especializados en esta área son pocos debido a la baja demanda de estos casos.

Fig.36. Número de peritos informáticos forense en Ecuador

Por otra parte, existen personas con buenas prácticas informática y uso de software, las mismas que hacen posible disminuir el impacto de este tipo de ataques a través de correos electrónicos o en el mejor de los casos no caer en este tipo de estafas y mitigarlo. He aquí la importancia de tener conocimientos sobre la estructura de estos ataques, sus tipos y funcionalidades.

Anexo 2

En el presente anexo se puede visualizar la definición de cada una de las etiquetas presentes en la estructura de un correo electrónico.

- **Received:** Estos campos son generados por los servidores de correo implicados en su transferencia.
- **From:** La etiqueta presenta información de la persona que envía el mensaje.
- **To:** Indica persona o personas a la que va dirigido el mensaje electrónico.
- **Subject:** Tema, título o asunto.
- **Thread-Topic:** El tema de un hilo de discusión.
- **Thread-Index:** Expone fecha y hora de envío el contenido del tag se encuentra codificado Base64.
- **Date:** Fecha y hora de envío
- **Message-ID:** Identificación individual compuesta por un código de cifras y letras y un nombre de dominio.
- **Accept-Language:** Destinado a especificar el idioma del usuario.
- **Content-Type:** Indica al cliente o navegador el tipo de archivo que se está enviando.
- **X-MS-Exchange-Organization-AuthAs:** Dirección que indica la procedencia del email y que se utiliza para procesar los rebotes de los correos electrónicos enviados desde la misma.

Anexo 3

ENCUESTA DIRIGIDA AL PERSONAL EDUCATIVO

La presente encuesta tiene como finalidad obtener estadísticas con relación a ciberataques y protección de los datos digitales

1. **¿Con qué frecuencia utiliza el servicio de correo electrónico?**

   - ◯ Diariamente
   - ◯ Más de tres días en la semana
   - ◯ Casi nunca

2. **Seleccione el servicio de correo electrónico que más utiliza.**

   - ◯ Gmail
   - ◯ Outlook
   - ◯ Yahoo
   - ◯ Otros

3. **Escoja una o varias opciones si es que conoce alguno de los siguientes ataques realizados a través de correos electrónicos**

   - ☐ Phishing
   - ☐ Malware
   - ☐ Apropiación de cuentas
   - ☐ Estafa
   - ☐ Otros
   - ☐ Ninguno

4. **¿Está usted consciente que los ciberdelincuentes pueden usar sus * datos personales para el cometimiento de delitos?**

   - ◯ Totalmente consciente
   - ◯ Medianamente consciente
   - ◯ Poco
   - ◯ Nada

5. **¿Alguna vez ha sido víctima de algún delito en el cual hayan obtenido de forma ilegal sus datos personales?**

- ◯ Si
- ◯ No

6. **En base a la pregunta anterior, seleccione el delito del que fue víctima.**

- ◯ Extorsión
- ◯ Acoso
- ◯ Suplantación de identidad
- ◯ Falsicación de Documentos
- ◯ Chantaje
- ◯ Otros
- ◯ Ninguno

7. **¿Qué método de seguridad informática utiliza para asegurar sus datos personales?**

- ◯ Antivirus
- ◯ Antispyware
- ◯ Firewall
- ◯ Anti-ransomware
- ◯ Identicador de Phishing
- ◯ Ninguno
- ◯ Otro

8. **A través de qué medio de información tuvo conocimientos sobre los ciberataques.**

- ◯ Televisión
- ◯ Redes Sociales
- ◯ Correo Electrónico
- ◯ Internet
- ◯ Otros
- ◯ Ninguno

9. **Si utiliza una o varias configuraciones de gestión o de clasificación de correo electrónico escoja una o varias opciones:**

- [ ] Firmas de página
- [ ] Creación de carpetas
- [ ] Respuestas Automáticas
- [ ] Gestión de documentos adjuntos
- [ ] Creación de etiquetas
- [ ] Ninguno

10. **¿Al momento de abrir un correo electrónico, se asegura de que el emisor de este mismo sea de confianza o conocido?**

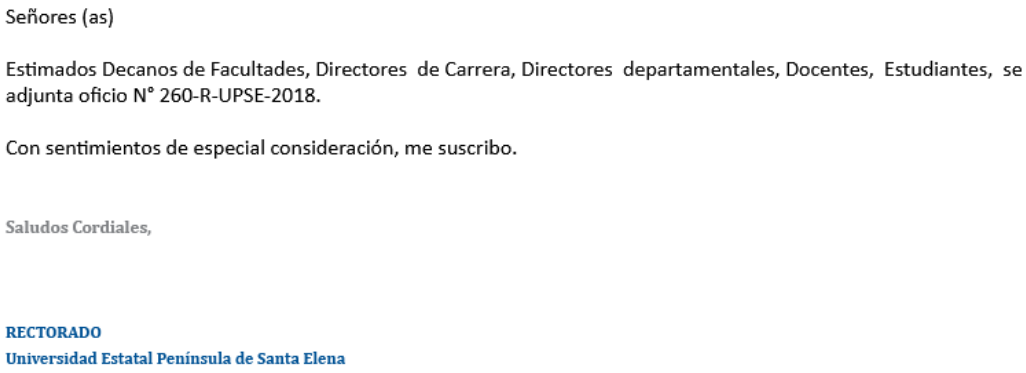
- ( ) Si
- ( ) Pocas veces No

Anexo 4

En el presente Anexo se detalla todo el proceso por fases del caso 1 (correo electrónico Zombie)

FASE DE ADQUISICIÓN

En el presente caso la persona que envía el correo electrónico trata de llamar la atención de un usuario del servicio de correo electrónico en el dominio de upse para que este descargue un archivo infectado con virus y se siga reproduciendo.


Señores (as)

Estimados Decanos de Facultades, Directores de Carrera, Directores departamentales, Docentes, Estudiantes, se adjunta oficio N° 260-R-UPSE-2018.

Con sentimientos de especial consideración, me suscribo.

Saludos Cordiales,

RECTORADO
Universidad Estatal Península de Santa Elena

Fig. 37. Correo electrónico Zombi

En la figura anterior se aprecia el archivo adjunto por el atacante que por medio de ingeniería social o engaños trata de convencer a su víctima para que esta lo descargue y así exponerse a los riesgos que este tipo de correo electrónico malicioso posee.

Fig.38. archivo adjunto del atancante

Mediante un análisis previo se puede observar el resultado de VirusTotal encontrando en este archivo alrededor de 6 tipos de virus insertados.

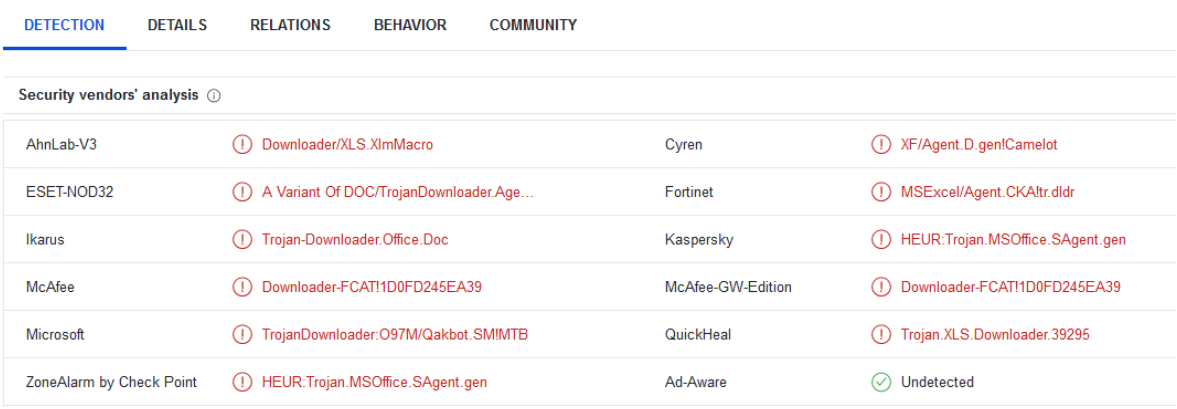


Fig. 39. Análisis realizado por Virus Total

FASE DE PRESERVACIÓN

En la presente fase el objetivo es adquirir el código hash codificado en SHA1 del presente experimento utilizando QFileHasher, obteniendo como resultado los siguientes caracteres pertenecientes al archivo en cuestión: **5913293ccad547840a07f72f9b2d5f890db80e0b**.

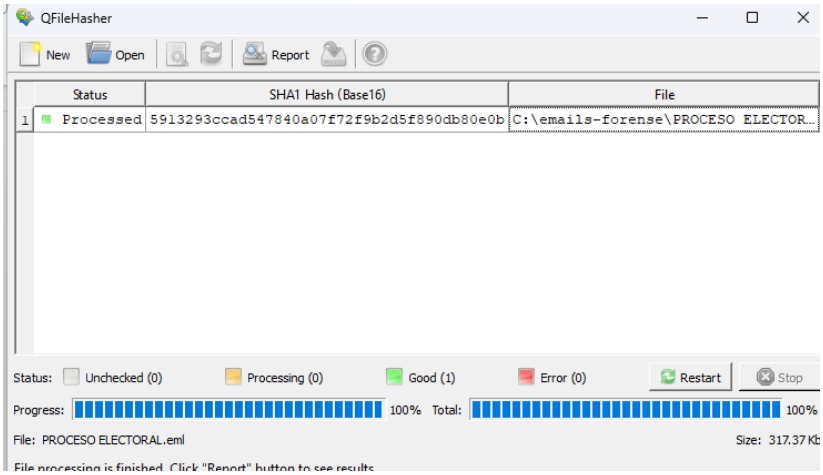


Fig. 40. Código hash Caso 1

FASE DE ANÁLISIS

Análisis de Cabecera

Se puede observar parte de lo que conforma la cabecera del correo electrónico analizado, en donde se aprecia que la etiqueta denominada “Received” se repite 4 veces, eso representa a los diferentes saltos que el mensaje electrónico dio antes de llegar a la

bandeja de entrada de la víctima, sin embargo, en estos saltos se encuentran asociadas 3 direcciones IP.

```
Received: from MWHPR17MB1519.namprd17.prod.outlook.com (2603:10b6:404:f7::32)
 by BN7PR17MB2051.namprd17.prod.outlook.com with HTTPS via
 BN6PR11CA0070.NAMPRD11.PROD.OUTLOOK.COM; Mon, 2 Jul 2018 22:01:33 +0000
Received: from MWHPR17MB1950.namprd17.prod.outlook.com (10.173.99.22) by
 MWHPR17MB1519.namprd17.prod.outlook.com (10.173.241.137) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.906.24; Mon, 2 Jul 2018 22:01:24 +0000
Received: from MWHPR17MB1357.namprd17.prod.outlook.com (10.173.104.15) by
 MWHPR17MB1950.namprd17.prod.outlook.com (10.173.99.22) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.906.23; Mon, 2 Jul 2018 22:00:40 +0000
Received: from MWHPR17MB1357.namprd17.prod.outlook.com
 ([fe80::692d:8d2e:1cb0:b5c9]) by MWHPR17MB1357.namprd17.prod.outlook.com
 ([fe80::692d:8d2e:1cb0:b5c9%4]) with mapi id 15.20.0906.026; Mon, 2 Jul 2018
 22:00:39 +0000
```

Fig.41. Cabecera de un correo electrónico

Mediante estos saltos realizados por el mensaje electrónico enviado, se presume que la primera IP expresada como “10.173.99.22” es la IP del presunto delincuente debido a que fue ahí de donde salió el correo electrónico. Con este número de IP se puede obtener una posible ubicación de la persona que envió el correo electrónico mediante la herramienta en Línea denominada “NordVPN”.

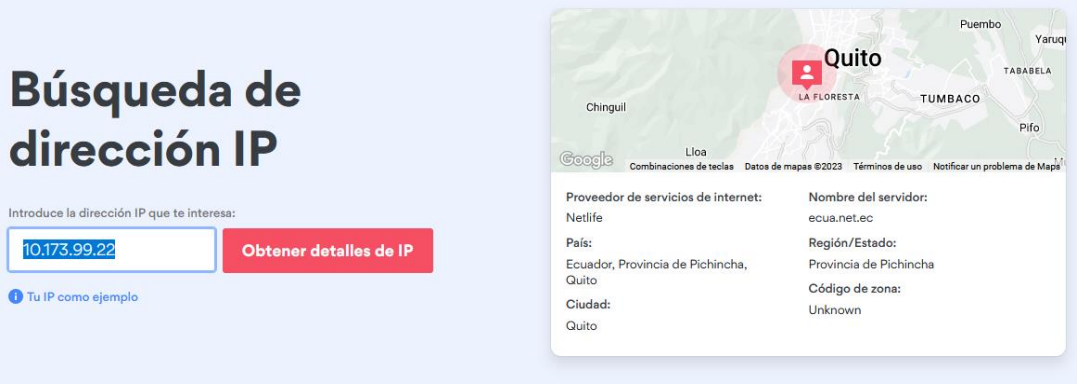


Fig.42. Ubicación y posibles coordenadas del atacante

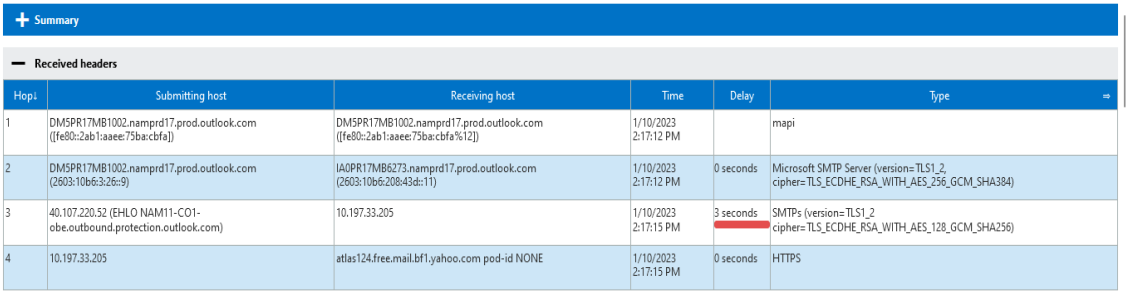
Otros ítems relacionados con la cabecera de un correo electrónico son los siguientes: From, To, Subject, Thread Topic, Thread Index, Date y Message – ID. Estas etiquetas también brindan información importante para la investigación, sin embargo, la etiqueta a destacar es la denominada como Thread-Index y Date. Mediante una investigación se

puede llegar a la conclusión de que lo antes mencionado brinda la misma información con la diferencia de que la etiqueta Thread-Index tiene cifrado los datos de la fecha de envío.

```
From: "Upse, Rectorado" <rectorado@upse.edu.ec>
To: DECANOS <decanos@upse.edu.ec>, DIRECTORES DE CARRERAS
        <directores_carreras@upse.edu.ec>, Directores Administrativos
        <directores_administrativos@upse.edu.ec>, DOCENTES <docentes@upse.edu.ec>,
        Estudiantes UPSE <estudiantes@upse.edu.ec>
Subject: PROCESO ELECTORAL
Thread-Topic: PROCESO ELECTORAL
Thread-Index: AQHUEk75pkdHFJKVwUOf1OtGgXtSDg==
Date: Mon, 2 Jul 2018 22:00:39 +0000
Message-ID:
        <MWHPR17MB13570D0602E585352B2626A5EC430@MWHPR17MB1357.namprd17.prod.outlook.com>
```

Fig.43. Estructura de cabecera

A continuación, se muestra el uso de otra herramienta para análisis de cabeceras de correos electrónicos en donde muestra la información resumida de la cabecera de una manera más detallada para el análisis a realizar. Se puede apreciar el número de saltos dado por el mensaje de correo electrónico junto con direcciones MAC, hora y fecho de los dispositivos que recibieron y enviaron el correo electrónico tipo phishing. Mediante esta información se sigue los pasos que realizó el correo electrónico hasta llegar a su destino.



Summary

Received headers

Hop	Submitting host	Receiving host	Time	Delay	Type
1	DM5PR17MB1002.namprd17.prod.outlook.com ([fe80::2ab1:aaee:75ba:cbfa])	DM5PR17MB1002.namprd17.prod.outlook.com ([fe80::2ab1:aaee:75ba:cbfa%12])	1/10/2023 2:17:12 PM		mapi
2	DM5PR17MB1002.namprd17.prod.outlook.com (2603:10b6:3:26::9)	IA0PR17MB6273.namprd17.prod.outlook.com (2603:10b6:208:43d::11)	1/10/2023 2:17:12 PM	0 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
3	40.107.220.52 (EHLO NAM11-CO1-obe.outbound.protection.outlook.com)	10.197.33.205	1/10/2023 2:17:15 PM	3 seconds	SMTPs (version=TLS1_2 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256)
4	10.197.33.205	atlas124.free.mail.bf1.yahoo.com pod-id NONE	1/10/2023 2:17:15 PM	0 seconds	HTTPS

Fig. 44. Análisis realizado por Message Header Analyzer Azure

Cuerpo

En esta sección se puede encontrar todo el contenido del mensaje visible relacionado con el correo electrónico, el correo electrónico tiene adjunto un archivo y este mismo tiene un malware, por lo tanto, es necesario encontrar el código dañino en el archivo recibido.

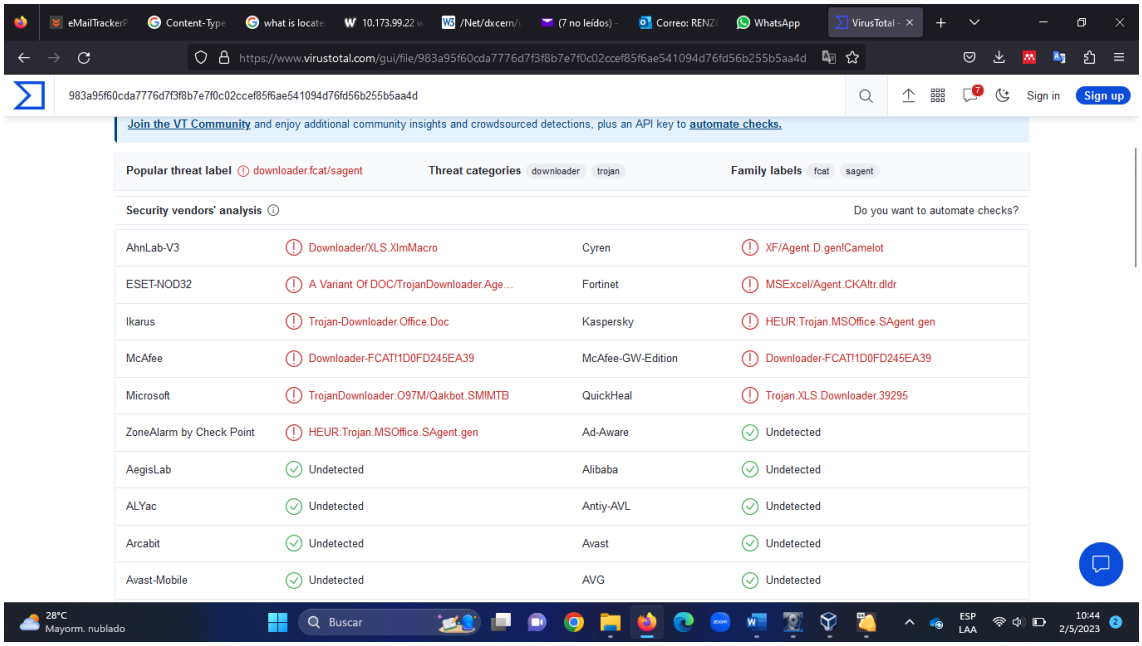


Fig. 45. Análisis del archivo adjunto

Anexo 5

En el presente Anexo se detalla todo el proceso por fases del experimento 2 (Phishing)

Fase de Adquisición

En este tipo de correos electrónicos el atacante trata de hacerse pasar por otra persona o institución con la finalidad de que la víctima ingrese al enlace proporcionado adjuntando un supuesto mensaje que sirve como detonante para que una persona entre en desesperación por en este caso "recuperar su cuenta" entrando al enlace que fue adjunto en mensaje electrónico y registre su información para que esta esté comprometida. En la siguiente imagen se puede ver el plagio de un correo electrónico del Banco Pichincha.

Fig.46. Phishing de un correo electrónico

En la siguiente evidencia se aprecia el link adjunto por el atacante que por medio de ingeniería social trata de convencer a su víctima para que esta ingrese y así exponerse a los riesgos que este tipo de correo electrónico malicioso posee.

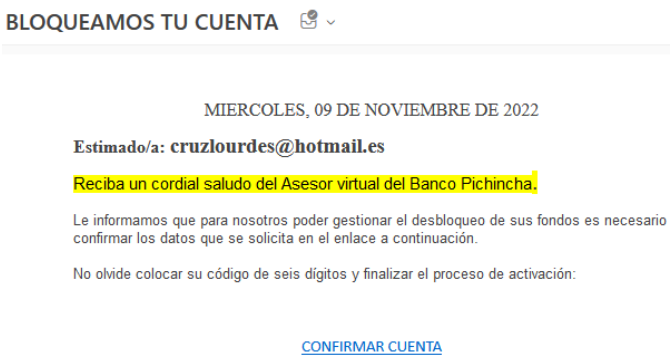


Fig.47. Enlace adjunto en el correo electrónico

Cuando la víctima entra al enlace el navegador advierte sobre el sitio que puede ser engañoso, sin embargo, si se acepta proseguir a visitar el enlace lo que aparecerá es una replica exacta de la página del login del Banco Pichincha y es ahí en donde la víctima ingresa sus datos bancarios y al enviarlos estarán comprometidos. Usando la herramienta de Virus Total se procede a analizar el enlace adjunto danto como resultado que la página es clasificada como phishing.

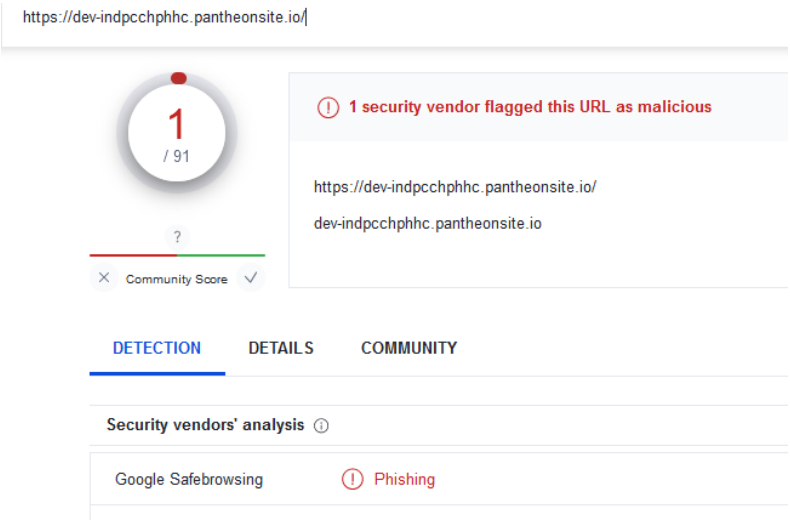


Fig.48. Resultado de Virus Total

FASE DE PRESERVACIÓN

En la presente fase el objetivo es adquirir el código hash codificado en MD5 del presente experimento utilizando QFileHasher, obteniendo como resultado los siguientes caracteres pertenecientes al archivo en cuestión: **ac815393ab14e419404cabc9970cce74650a803d**.

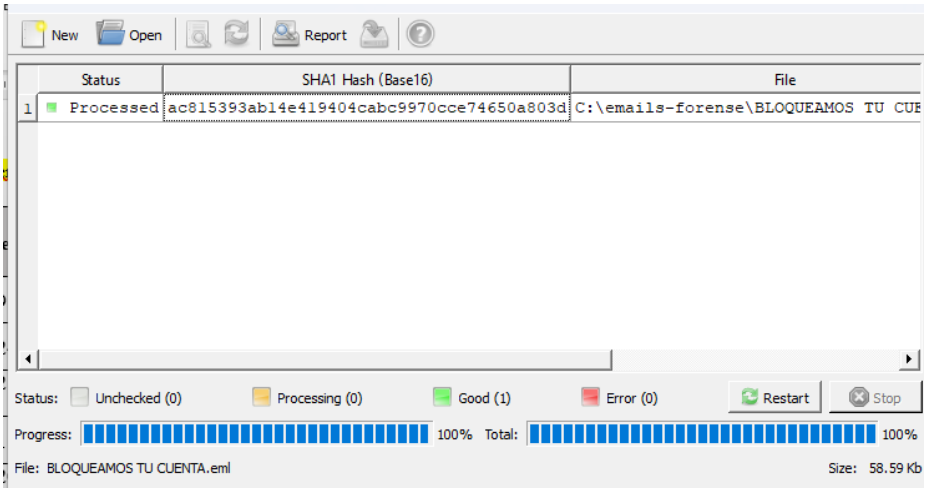
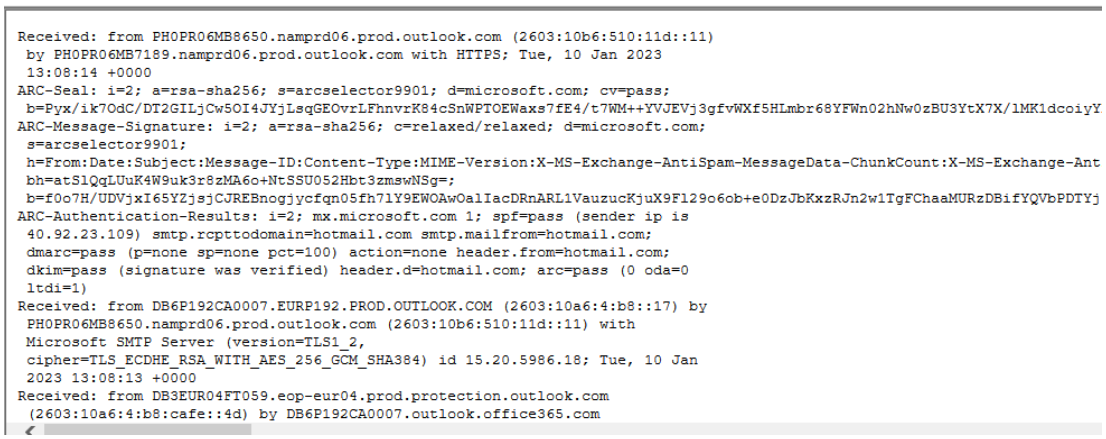


Fig.49. Código hash para el caso 2

FASE DE ANÁLISIS

Análisis de Cabecera

Este caso posee una gran cantidad de información dentro de la cabera, se puede notar por la etiqueta “Received” que hizo varios saltos para llegar al destino, para ser más específicos dio un total de 6 saltos. Sin embargo de esta información se pudo rescatar 2 direcciones IP, de la cual la siguiente 40.92.97.75 se presume es la dirección del posible delincuente.



```
Received: from PH0PR06MB8650.namprd06.prod.outlook.com (2603:10b6:510:11d::11)
 by PH0PR06MB7189.namprd06.prod.outlook.com with HTTPS; Tue, 10 Jan 2023
 13:08:14 +0000
ARC-Seal: i=2; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv=pass;
 b=Pyx/ik7OdC/DT2GILjCw5OI4JYjLsqGEOvrLFhnvrK84cSnWPTOEWaxs7fE4/t7WM++YVJEVj3gfvWXf5HLmbr68YFWn02hNw0zBU3YtX7X/lMK1dcoiyY
ARC-Message-Signature: i=2; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com;
 s=arcselector9901;
 h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-AntiSpam-MessageData-ChunkCount:X-MS-Exchange-Ant
 bh=atSlQqLUuK4W9uk3r8zMA6o+NtSSU052Hbt3zmswNSg=;
 b=f0o7H/UDVjxI65YZjsjCJREBnogjycfqn05fh7lY9EWOAwOalIacDRnARL1VauzucKjuX9Fl29o6ob+e0DzJbKxzRJn2w1TgFChaaMURzDBifYQVbPDTYj
ARC-Authentication-Results: i=2; mx.microsoft.com 1; spf=pass (sender ip is
 40.92.23.109) smtp.rcpttodomain=hotmail.com smtp.mailfrom=hotmail.com;
 dmarc=pass (p=none sp=none pct=100) action=none header.from=hotmail.com;
 dkim=pass (signature was verified) header.d=hotmail.com; arc=pass (0 oda=0
 ltdi=1)
Received: from DB6P192CA0007.EURP192.PROD.OUTLOOK.COM (2603:10a6:4:b8::17) by
 PH0PR06MB8650.namprd06.prod.outlook.com (2603:10b6:510:11d::11) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5986.18; Tue, 10 Jan
 2023 13:08:13 +0000
Received: from DB3EUR04FT059.eop-eur04.prod.protection.outlook.com
 (2603:10a6:4:b8:cafe::4d) by DB6P192CA0007.outlook.office365.com
```

Fig.50. Cabecera de un correo electrónico

Se requiere aprovechar de las huellas digitales de la persona en cuestión para encontrar al posible responsable, mediante la dirección IP proporcionada por la cabecera, se puede realizar un pequeño análisis como la anterior expuesta para obtener su posible ubicación. Como resultado del análisis se obtiene que este ataque se lo realizó desde la ciudad de Quito.

Fig.51. Posible ubicación del delincuente

Además de obtener la posible localización del atacante mediante las etiquetas hay que analizar el contenido del cuerpo del correo electrónico encontrando cualquier información de utilidad para la investigación. Lo que se puede observar es que tiene un correo electrónico personal "pau_reina@hotmail.com" en donde debería de ir el correo electrónico oficial de la agencia bancaria mencionada.

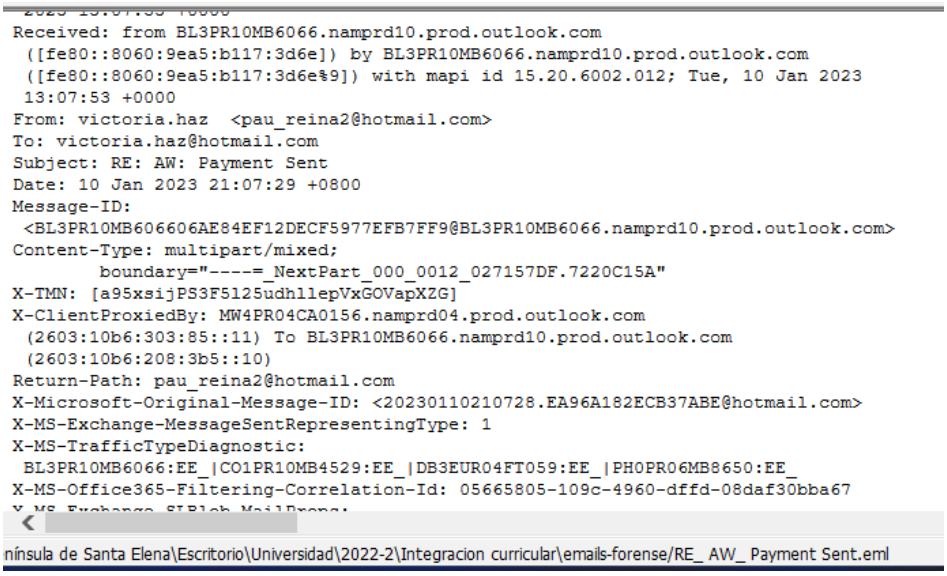
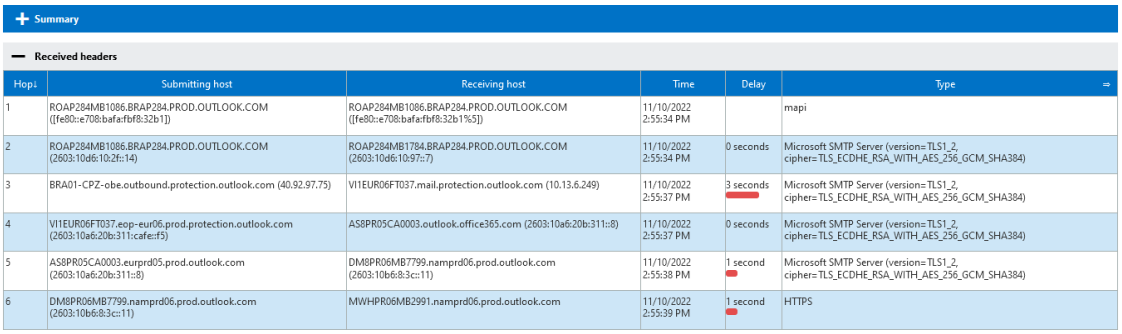


Fig.53. Cuerpo del correo electrónico caso 3

A continuación, se muestra el uso de otra herramienta para análisis de cabeceras de correos electrónicos en donde muestra la información resumida de la cabecera de una manera más detallada para el análisis a realizar. Se puede apreciar el número de saltos dado por el mensaje de correo electrónico junto con direcciones MAC, hora y fecho de los dispositivos que recibieron y enviaron el correo electrónico tipo phishing. Mediante esta información se sigue los pasos que realizó el correo electrónico hasta llegar a su destino.



Hop	Submitting host	Receiving host	Time	Delay	Type
1	ROAP284MB1086.BRAP284.PROD.OUTLOOK.COM ([fe80::e708:baf:fbf8:32b1])	ROAP284MB1086.BRAP284.PROD.OUTLOOK.COM ([fe80::e708:baf:fbf8:32b1%5])	11/10/2022 2:55:34 PM		mapi
2	ROAP284MB1086.BRAP284.PROD.OUTLOOK.COM (2603:10d6:10:2f::14)	ROAP284MB1784.BRAP284.PROD.OUTLOOK.COM (2603:10d6:10:97::7)	11/10/2022 2:55:34 PM	0 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
3	BRA01-CPZ-obe.outbound.protection.outlook.com (40.92.97.75)	VI1EUR06FT037.mail.protection.outlook.com (10.13.6.249)	11/10/2022 2:55:37 PM	3 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
4	VI1EUR06FT037.eop-eur06.prod.protection.outlook.com (2603:10a6:20b:311:cafe::f5)	AS8PR05CA0003.outlook.office365.com (2603:10a6:20b:311::8)	11/10/2022 2:55:37 PM	0 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
5	AS8PR05CA0003.eurprd05.prod.outlook.com (2603:10a6:20b:311::8)	DM8PR06MB7799.namprd06.prod.outlook.com (2603:10b6:8:3c::11)	11/10/2022 2:55:38 PM	1 second	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
6	DM8PR06MB7799.namprd06.prod.outlook.com (2603:10b6:8:3c::11)	MWHPR06MB2991.namprd06.prod.outlook.com	11/10/2022 2:55:39 PM	1 second	HTTPS

Fig.54. Análisis realizado por Message Header Analyzer Azure Caso 2

Cuerpo

En la presente sección se observa que el diseño del phishing relacionado con la institución bancaria “Banco Pichincha” es construido con html, es mismo que permite crear diseños personales para una página web.

Fig.55. Cuerpo del correo electrónico

Anexo 6

En el presente Anexo se detalla todo el proceso por fases del experimento 3 (Correo electrónico fraudulento)

FASE DE ADQUISIÓN

La finalidad que estos tipos de correos electrónicos poseen es que a travez de una mentira, amaneza o extorción hacen que las víctimas cumplan los objetivos del atacante, en el siguiente caso como se puede apreciar en el imagen el atacante por medio de una mentira adjunta una supuesta orden de captura generada por la interpol con el objetivo de que la víctima se comunique con el remitente y así proceder con la extorción.

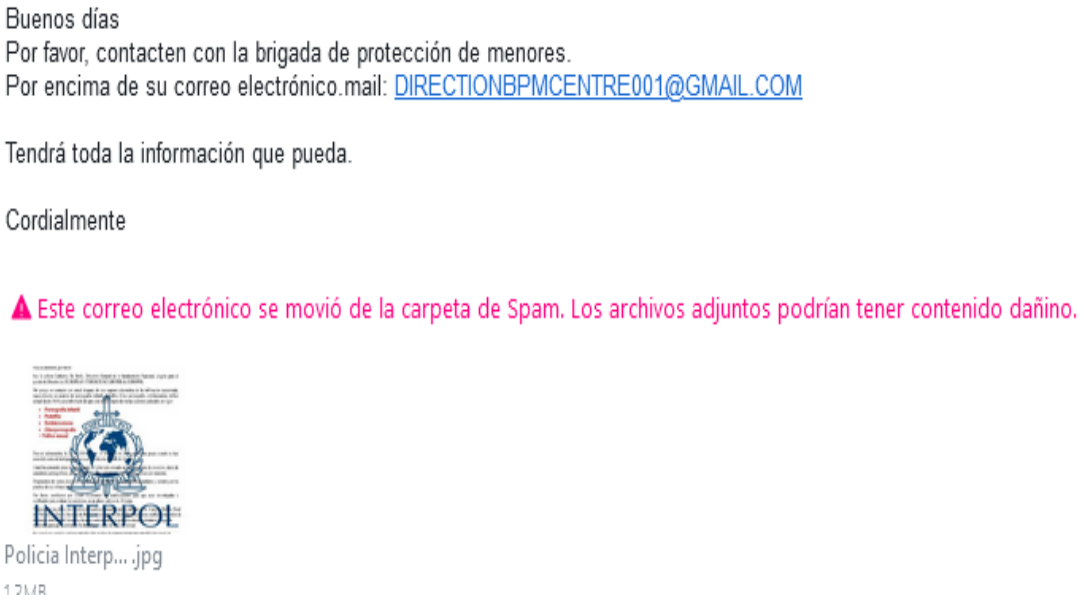


Fig.56. Correo electrónico extorsionador recibido

Antes de abrir la imagen adjunta es necesario poder analizarla utilizando un software o algoritmo confiable, por preferencia se usa Virus Total en donde en la Figura 9 arroja el resultado de que no presenta ningún tipo de virus por lo que es seguro abrirlo y examinar su contenido.

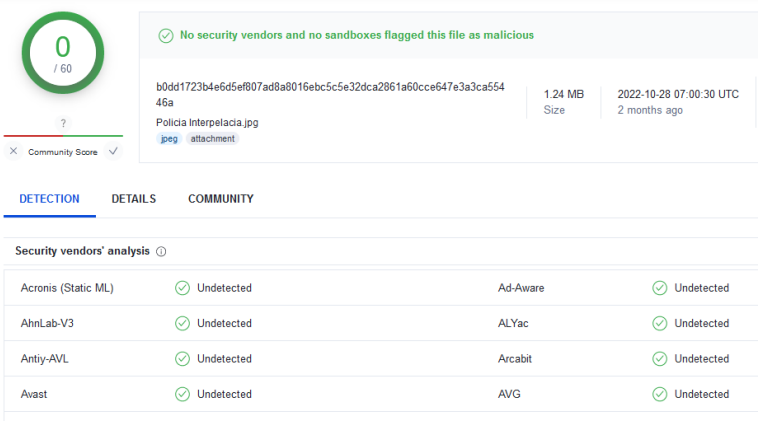


Fig.57. Resultado de análisis de Virus Total

FASE DE PRESERVACIÓN

En la presente fase el objetivo es adquirir el código hash codificado en MD5 del presente experimento utilizando QFileHasher, obteniendo como resultado los siguientes caracteres pertenecientes al archivo en cuestión: **f3c9f671d09b0ecd4fcbf87dbca973b9baa39305**.

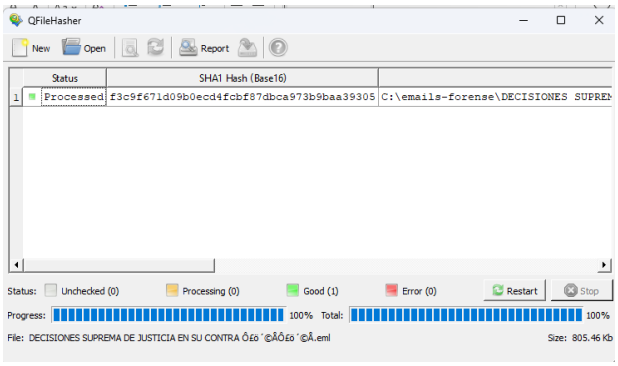


Fig.58. Código hash para el caso 3

FASE DE ANALISIS

Cabecera

Al igual que los casos anteriores se encuentra evidencia de los diferentes saltos realizados por el mensaje de correo electrónico, en este caso se puede apreciar que el número de saltos realizado por el correo electrónico es un total de 5 para llegar al destino. En donde se puede encontrar la siguiente dirección IP 209.85.221.45, la misma que se presume es de la persona que realiza este ataque a través de correo electrónico.

```
Received: from PH0PR06MB7753.namprd06.prod.outlook.com (::1) by
 PH0PR06MB7189.namprd06.prod.outlook.com with HTTPS; Tue, 6 Dec 2022 12:24:44
 +0000
Received: from BN0PR04CA0078.namprd04.prod.outlook.com (2603:10b6:408:ea::23)
 by PH0PR06MB7753.namprd06.prod.outlook.com (2603:10b6:510:e3::23) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5880.11; Tue, 6 Dec
 2022 12:24:42 +0000
Received: from BN8NAM04FT047.eop-NAM04.prod.protection.outlook.com
 (2603:10b6:408:ea:cafe::54) by BN0PR04CA0078.outlook.office365.com
 (2603:10b6:408:ea::23) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5880.14 via Frontend
 Transport; Tue, 6 Dec 2022 12:24:42 +0000
Authentication-Results: spf=pass (sender IP is 209.85.221.45)
 smtp.mailfrom=gmail.com; dkim=pass (signature was verified)
 header.d=gmail.com;dmarc=pass action=none header.from=gmail.com;compauth=pass
 reason=100
Received-SPF: Pass (protection.outlook.com: domain of gmail.com designates
```

Fig. 59. Saltos realizados por el correo electrónico

Por otra parte, cada uno de estos saltos al igual que los casos anteriores, nos proporciona las direcciones IP y MAC de los saltos que este hizo, por lo tanto, es conveniente analizar el primero para conocer la posible ubicación del delincuente. Como resultado del intento de encontrar la dirección es que el atacante reside en un estado llamado “KANSAS”.

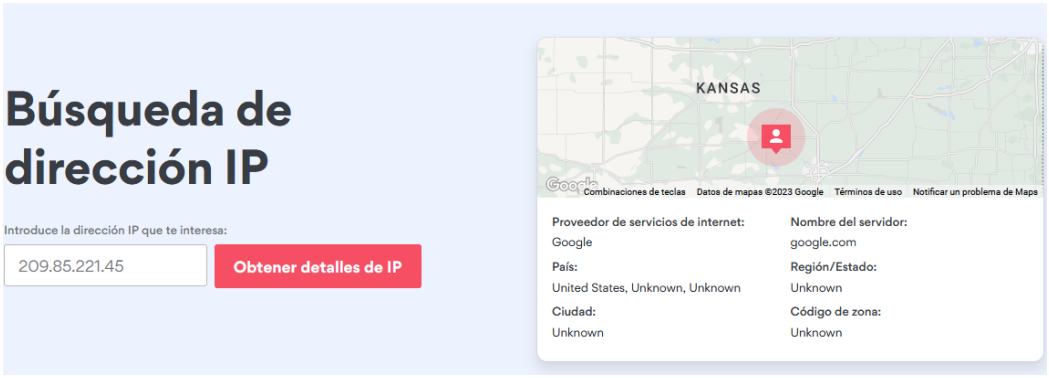


Fig.60. Posible dirección del atacante

Para este caso específico se puede encontrar relacionado 2 direcciones de correos electrónicos como sospechosos debido a que no pertenecen al receptor de la información en este caso victoria.haz@hotmail.com, sin embargo, los siguientes: espagnoljudicialpolicia@gmail.com y yeoissa2019@hotmail.com son los implicados como sospechosos.

```
From: "suprÃªme Justicia" <espagnoljudicialpolicia@gmail.com>
Date: Tue, 6 Dec 2022 12:21:28 +0100
Message-ID: <CAOgSvMRftrJiBrSu7Qo5R0g8JQEgRFtS8Ksu0e9t5P7M9DQJzg@mail.gmail.com>
Subject: DECISIONES SUPREMA DE JUSTICIA EN SU CONTRA âœ"ï¸âœ"ï¸
To: citaciÃ³n@gouv.fr
Content-Type: multipart/mixed; boundary="0000000000065340b05ef27e353"
Bcc: victoria.haz@hotmail.com
X-IncomingHeaderCount: 16
Return-Path: yeoissa2019@gmail.com
X-MS-Exchange-Organization-ExpirationStartTime: 06 Dec 2022 12:24:42.3000
```

Fig.61. Etiquetas de la cabecera

A continuación, se muestra el uso de otra herramienta para análisis de cabeceras de correos electrónicos en donde muestra la información resumida de la cabecera de una manera más detallada para el análisis a realizar. Se puede apreciar el número de saltos dado por el mensaje de correo electrónico junto con direcciones MAC, hora y fecho de los dispositivos que recibieron y enviaron el correo electrónico tipo phishing. Mediante esta información se sigue los pasos que realizó el correo electrónico hasta llegar a su destino.

+ Summary

− Received headers

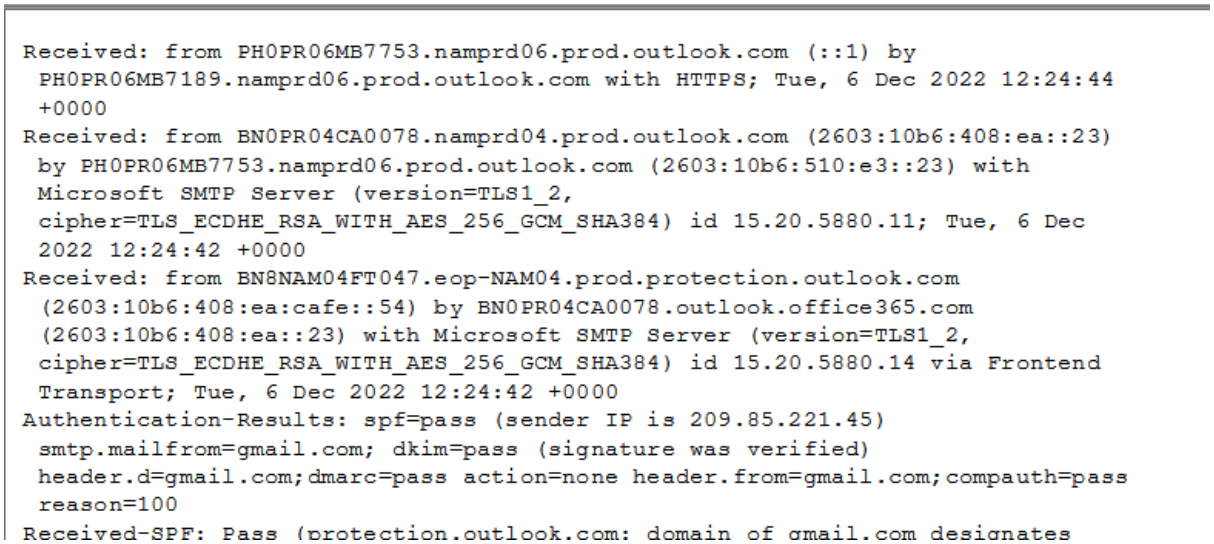
Hop↓	Submitting host	Receiving host	Time	Delay	Type
1		mail-wr1-f45.google.com	12/6/2022 7:24:42 AM		SMTP
2	mail-wr1-f45.google.com (209.85.221.45)	BN8NAM04FT047.mail.protection.outlook.com (10.13.161.34)	12/6/2022 7:24:42 AM	0 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
3	BN8NAM04FT047.eop-NAM04.prod.protection.outlook.com (2603:10b6:408:ea:cafe::54)	BN0PR04CA0078.outlook.office365.com (2603:10b6:408:ea::23)	12/6/2022 7:24:42 AM	0 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
4	BN0PR04CA0078.namprd04.prod.outlook.com (2603:10b6:408:ea::23)	PH0PR06MB7753.namprd06.prod.outlook.com (2603:10b6:510:e3::23)	12/6/2022 7:24:42 AM	0 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
5	PH0PR06MB7753.namprd06.prod.outlook.com (::1)	PH0PR06MB7189.namprd06.prod.outlook.com	12/6/2022 7:24:44 AM	2 seconds	HTTPS

Fig.61. Etiquetas de la cabecera Análisis realizado por Message Header Analyzer Azure

Caso 3

Cuerpo

En el cuerpo de este correo electrónico se puede encontrar el archivo adjunto denominado como “Convocatoria”, el mismo que contiene un mensaje que sirve para llamar la atención de la víctima.



```
Received: from PH0PR06MB7753.namprd06.prod.outlook.com (::1) by
 PH0PR06MB7189.namprd06.prod.outlook.com with HTTPS; Tue, 6 Dec 2022 12:24:44
 +0000
Received: from BN0PR04CA0078.namprd04.prod.outlook.com (2603:10b6:408:ea::23)
 by PH0PR06MB7753.namprd06.prod.outlook.com (2603:10b6:510:e3::23) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5880.11; Tue, 6 Dec
 2022 12:24:42 +0000
Received: from BN8NAM04FT047.eop-NAM04.prod.protection.outlook.com
 (2603:10b6:408:ea:cafe::54) by BN0PR04CA0078.outlook.office365.com
 (2603:10b6:408:ea::23) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5880.14 via Frontend
 Transport; Tue, 6 Dec 2022 12:24:42 +0000
Authentication-Results: spf=pass (sender IP is 209.85.221.45)
 smtp.mailfrom=gmail.com; dkim=pass (signature was verified)
 header.d=gmail.com;dmarc=pass action=none header.from=gmail.com;compauth=pass
 reason=100
Received-SPF: Pass (protection.outlook.com: domain of gmail.com designates
```

Fig.62. Saltos realizados por el correo electrónico

Anexo 7

En el presente Anexo se detalla todo el proceso por fases del experimento 4 (Correo electrónico Malware).

FASE DE ADQUISICIÓN

Los correos electrónicos con malware se caracterizan por poseer un archivo malicioso adjunto, enlace a una página fraudulenta dentro de estos mismos, las motivaciones para realizar este tipo de ataques son variadas tanto así que pueden ir desde una simple broma, prueba de las habilidades o hasta capturar datos personales o infectar servidores de una empresa en específico y así tener un beneficio económico. A continuación, se presenta un mensaje de correo electrónico con un malware adjunto.

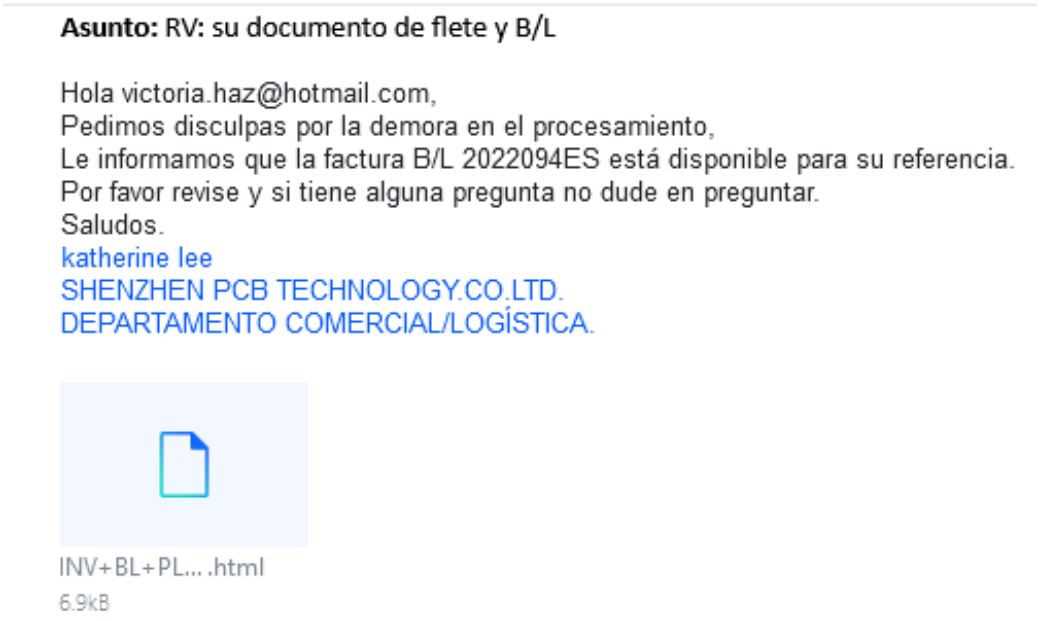


Fig.63. Correo electrónico con Malware Troyano

El archivo adjunto en el correo electrónico es una supuesta factura dirigida a un cliente sin embargo mediante un análisis rápido del documento mediante virus total da como resultado que el archivo contiene un virus troyano además de que posee enlaces a una pagina web que utiliza un método popular de phishing.

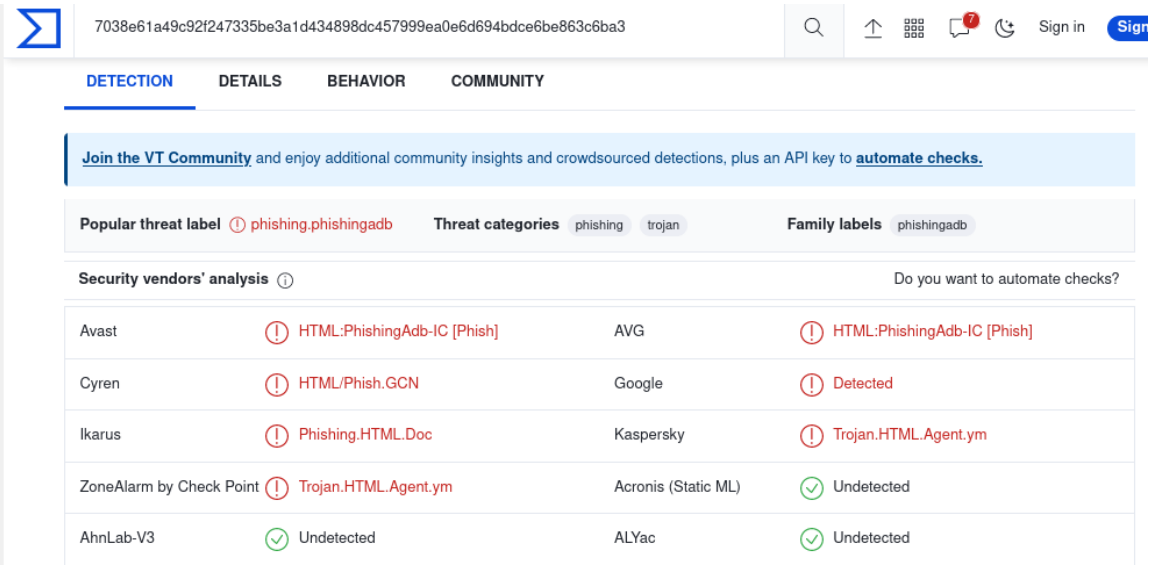


Fig.64. Análisis del archivo adjunto

FASE DE PRESERVACIÓN

En la presente fase el objetivo es adquirir el código hash codificado en MD5 del presente experimento utilizando QFileHasher, obteniendo como resultado los siguientes caracteres pertenecientes al archivo en cuestión: **22840df8e8843cd4b9b1fbcf04864b0b27ac168c.**

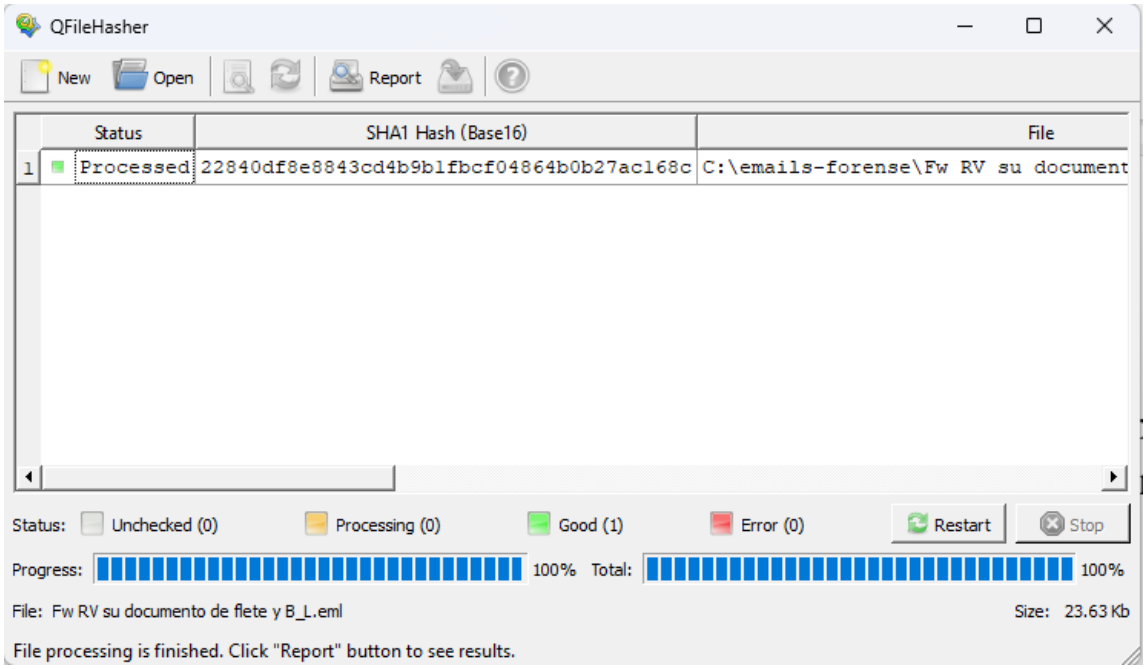


Fig.65. Código hash para el caso 4

FASE DE ANALISIS

Cabecera

Al igual que los casos anteriores se encuentra evidencia de los diferentes saltos realizados por el mensaje de correo electrónico, en este caso se puede apreciar que el número de saltos realizado por el correo electrónico es un total de 7 para llegar al destino. En donde se puede encontrar la siguiente dirección IP 190.15.141.157, la misma que se presume es de la persona que realiza este ataque a través de correo electrónico.

```
Received: from DS7PR17MB6609.namprd17.prod.outlook.com (2603:10b6:8:ea::18) by
 SN6PR17MB2527.namprd17.prod.outlook.com with HTTPS; Thu, 22 Jun 2023 14:36:42
 +0000
Received: from MW4PR03CA0006.namprd03.prod.outlook.com (2603:10b6:303:8f::11)
 by DS7PR17MB6609.namprd17.prod.outlook.com (2603:10b6:8:ea::18) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6521.24; Thu, 22 Jun
 2023 14:36:39 +0000
Received: from MW2NAM10FT040.eop-nam10.prod.protection.outlook.com
 (2603:10b6:303:8f:cafe::5f) by MW4PR03CA0006.outlook.office365.com
 (2603:10b6:303:8f::11) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6521.24 via Frontend
 Transport; Thu, 22 Jun 2023 14:36:38 +0000
Authentication-Results: spf=neutral (sender IP is 190.15.141.157)
 smtp.mailfrom=yahoo.com; dkim=pass (signature was verified)
 header.d=yahoo.com;dmarc=pass action=none header.from=yahoo.com;compauth=pass
 reason=100
```

Fig.66. Saltos realizados por el correo electrónico

Por otra parte, cada uno de estos saltos al igual que los casos anteriores, nos proporciona las direcciones IP y MAC de los saltos que este hizo, por lo tanto, es conveniente analizar el primero para conocer la posible ubicación del delincuente. Como resultado del intento de encontrar la dirección es que el atacante realizó la actividad ilícita desde la Provincia de Manabí.

IP address	**190.15.141.157** (change)
Latitude	-0.9635
Longitude	-80.7144
Country	Ecuador
Region	Provincia de Manabi
City	Manta
Organization	CEDIA

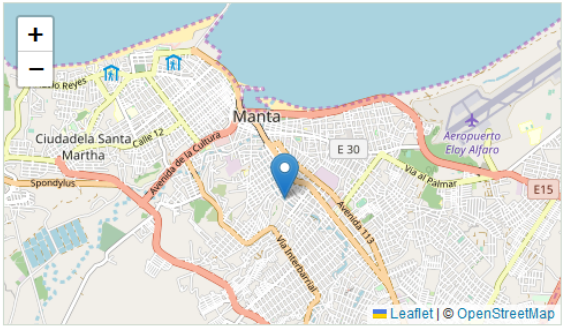
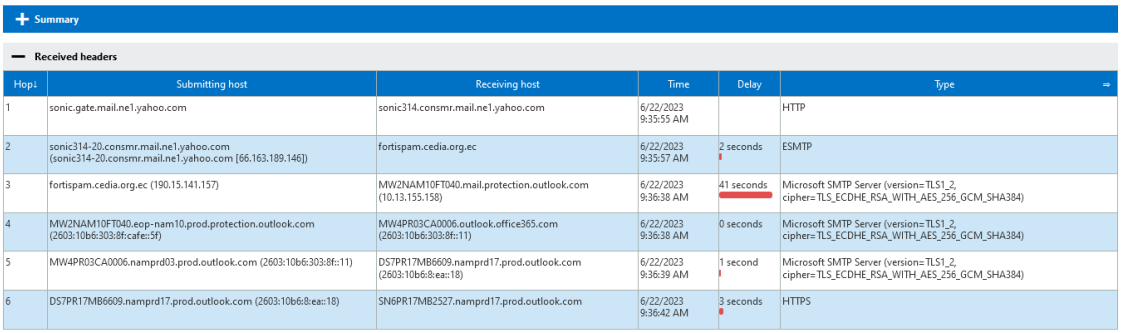


Fig.67. Posible ubicación del ciberdelincuente

A continuación, se muestra el uso de otra herramienta para análisis de cabeceras de correos electrónicos en donde muestra la información resumida de la cabecera de una manera más detallada para el análisis a realizar. Se puede apreciar el número de saltos dado por el mensaje de correo electrónico junto con direcciones MAC, hora y fecho de los dispositivos que recibieron y enviaron el correo electrónico tipo phishing. Mediante esta información se sigue los pasos que realizó el correo electrónico hasta llegar a su destino.



Summary

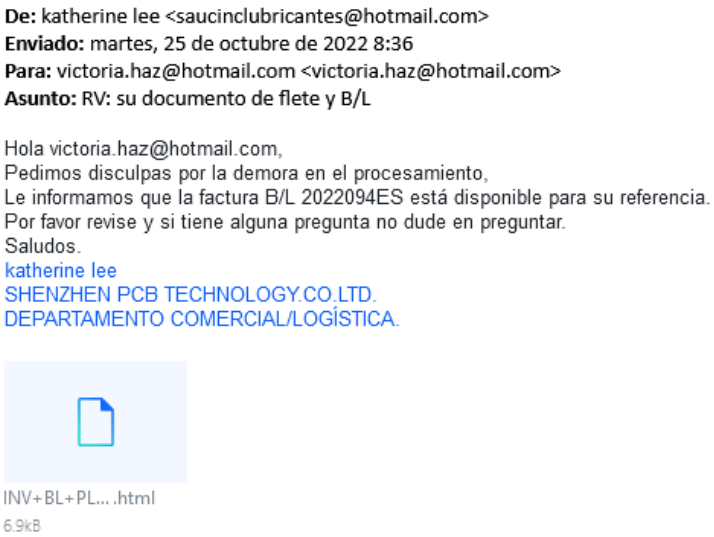
Received headers

Hop	Submitting host	Receiving host	Time	Delay	Type
1	sonic.gate.mail.ne1.yahoo.com	sonic314.consmr.mail.ne1.yahoo.com	6/22/2023 9:35:55 AM		HTTP
2	sonic314-20.consmr.mail.ne1.yahoo.com (sonic314-20.consmr.mail.ne1.yahoo.com [66.163.189.146])	fortispam.cedia.org.ec	6/22/2023 9:35:57 AM	2 seconds	ESMTP
3	fortispam.cedia.org.ec (190.15.141.157)	MW2NAM10FT040.mail.protection.outlook.com (10.13.155.158)	6/22/2023 9:36:38 AM	41 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
4	MW2NAM10FT040.eop-nam10.prod.protection.outlook.com (2603:10b6:303:8f:cafe::5f)	MW4PR03CA0006.outlook.office365.com (2603:10b6:303:8f::11)	6/22/2023 9:36:38 AM	0 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
5	MW4PR03CA0006.namprd03.prod.outlook.com (2603:10b6:303:8f::11)	DS7PR17MB6609.namprd17.prod.outlook.com (2603:10b6:8:ea::18)	6/22/2023 9:36:39 AM	1 second	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
6	DS7PR17MB6609.namprd17.prod.outlook.com (2603:10b6:8:ea::18)	SN6PR17MB2527.namprd17.prod.outlook.com	6/22/2023 9:36:42 AM	3 seconds	HTTPS

Fig.68. Etiquetas de la cabecera Análisis realizado por Message Header Analyzer Azure Caso 4

Cuerpo

En el cuerpo de este correo electrónico se puede encontrar un mensaje corto con la finalidad de llamar la atención del usuario para poder descargar el archivo infectado que está adjunto.



De: katherine lee <saucinclubricantes@hotmail.com>
Enviado: martes, 25 de octubre de 2022 8:36
Para: victoria.haz@hotmail.com <victoria.haz@hotmail.com>
Asunto: RV: su documento de flete y B/L

Hola victoria.haz@hotmail.com,
Pedimos disculpas por la demora en el procesamiento,
Le informamos que la factura B/L 2022094ES está disponible para su referencia.
Por favor revise y si tiene alguna pregunta no dude en preguntar.
Saludos.
katherine lee
SHENZHEN PCB TECHNOLOGY.CO.LTD.
DEPARTAMENTO COMERCIAL/LOGÍSTICA.

INV+BL+PL... .html
6.9kB

Fig.69. Mensaje de correo electrónico

Anexo 8

En el presente Anexo se detalla todo el proceso por fases del experimento 5 (Correo electrónico Autoenvío).

FASE DE ADQUISICIÓN

Se puede observar que en la bandeja de entrada de la víctima existe un mensaje muy particular, el cual supuestamente se lo envió así mismo, según lo mostrado en su correo electrónico, sin embargo, el asunto y el cuerpo del mensaje poseen un tipo de escritura extraña, pero de cierta manera entendible.

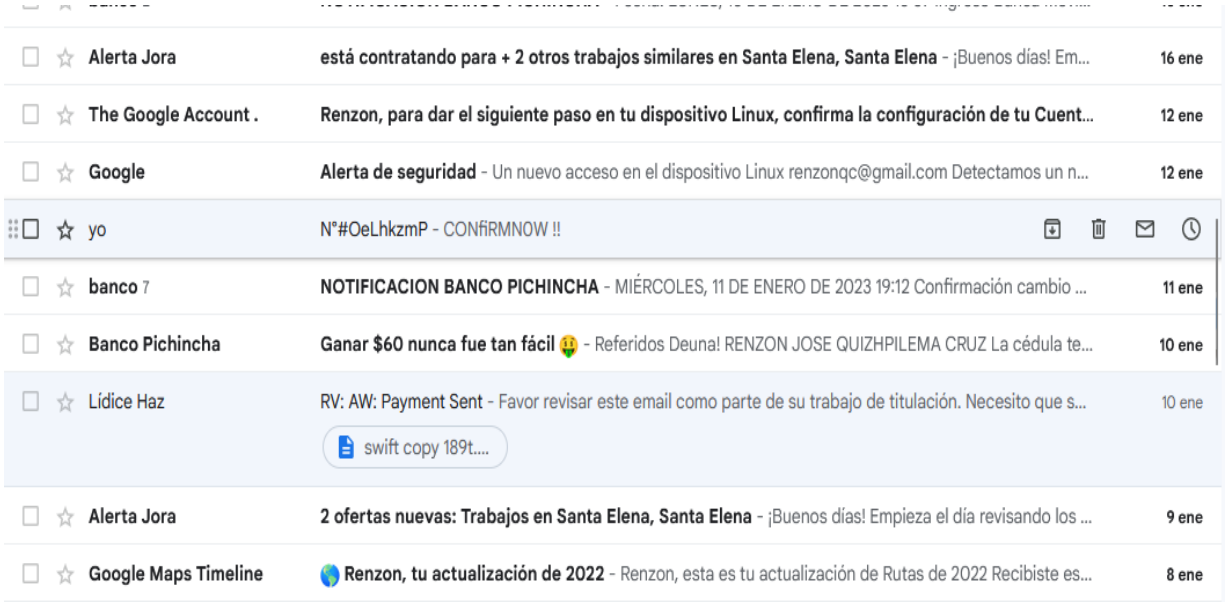


Fig.70. Bandeja de entrada de la víctima

Dentro del mensaje tratado se puede observar que la imagen que identifica al perfil que envía el mensaje es el mismo que el de la víctima, además este correo electrónico consta de una imagen con texto en el idioma inglés, además de poseer un link sospechoso debido a su tipo de escritura.

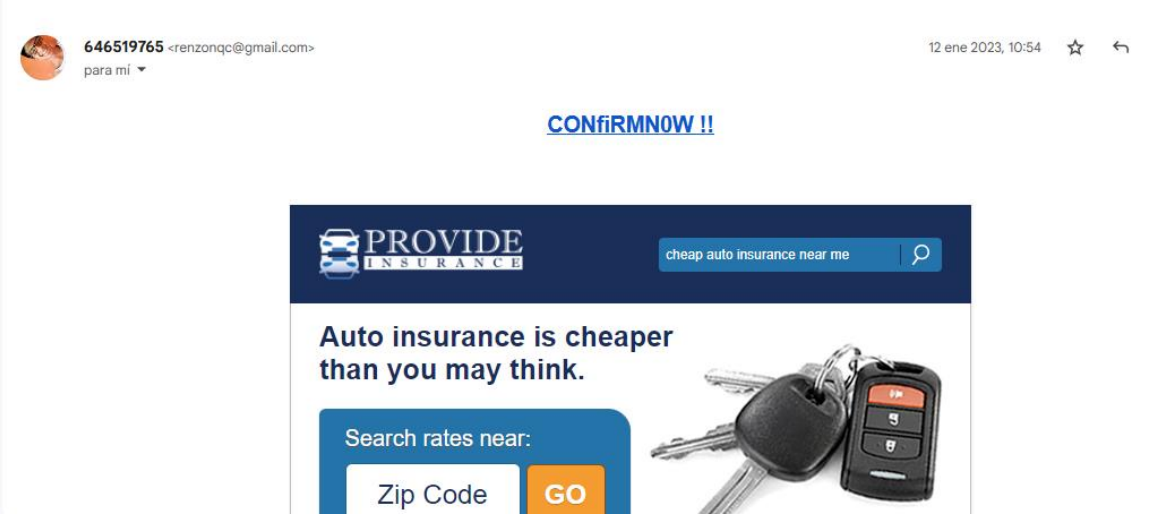


Fig.71. Mensaje de correo electrónico ingeniería social

Mediante un análisis al link proporcionado en el correo electrónico a través de virus total se puede observar que aparentemente el link no está infectado con ningún tipo de malware y tampoco consta como un intento de phishing.

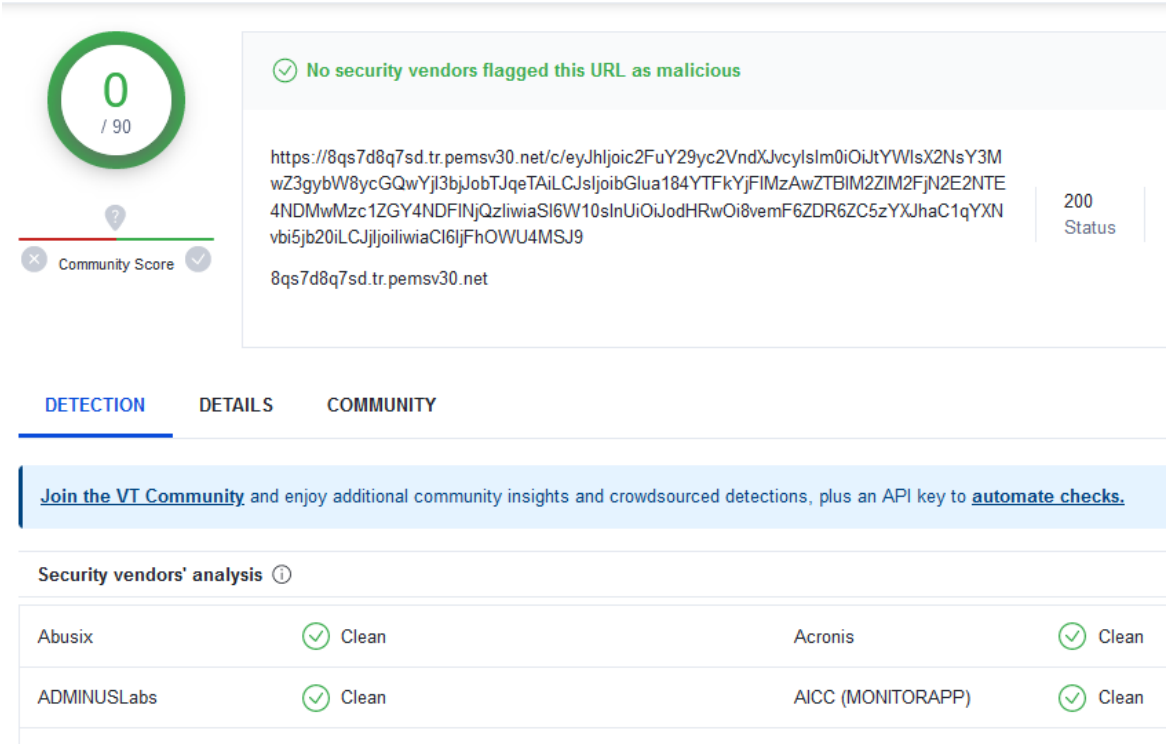


Fig.72. Análisis con Virus Total

FASE DE PRESERVACIÓN

En la presente fase el objetivo es adquirir el código hash codificado en MD5 del presente experimento utilizando QFileHasher, obteniendo como resultado los siguientes caracteres pertenecientes al archivo en cuestión: **8300eae3435bc2caf249d7eab994a887a6e8ea1e.**

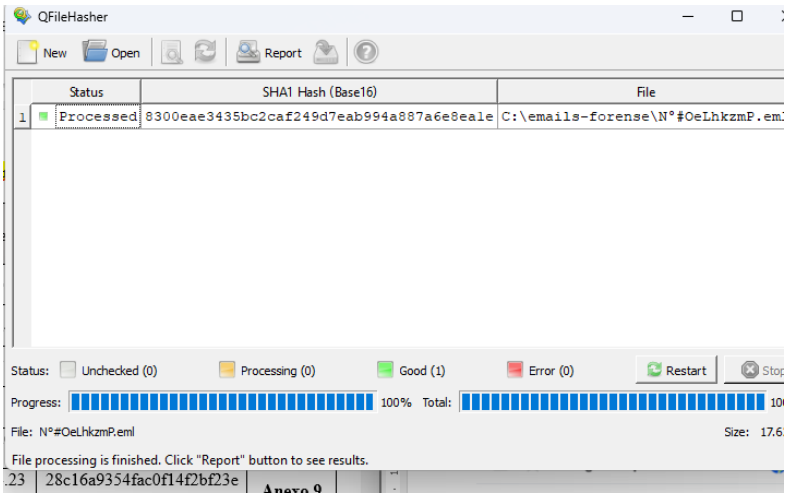


Fig.73. Código hash para el caso 5

FASE DE ANALISIS

Cabecera

Al igual que los casos anteriores se encuentra evidencia de los diferentes saltos realizados por el mensaje de correo electrónico, en este caso se puede apreciar que el número de saltos realizado por el correo electrónico es un total de 5 para llegar al destino. En donde se puede encontrar la siguiente dirección IP 209.85.202.101 la misma que se presume es de la persona que realiza este ataque a través de correo electrónico.

```
Delivered-To: renzonqc@gmail.com
Received: by 2002:ac4:9303:0:b0:58a:95f4:7b15 with SMTP id k3csp5141180pii;
        Thu, 12 Jan 2023 07:54:17 -0800 (PST)
X-Received: by 2002:a17:907:6746:b0:836:e7de:9792 with SMTP id qm6-20020a170907674600b00836e7de9792
        Thu, 12 Jan 2023 07:54:16 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1673538856; cv=none;
        d=google.com; s=arc-20160816;
        b=BAV4Xc40+YAO5TULf5MZrN6BQ1duTPhvQb5oL2EW3VCc9elbVrGbkF9jR4nrZDHrlj
         PpVuLyvPNywMpaSF14hzMK8j4pZCmXvFLDZVVBsMytmW5hRYYJ++k7yulGvJtnfCS3Uw
         kjaMtefwI8hlOxp7HMHK3b4NlJJbR94DSsVy5LBpBc+VzZn6KV2zDtUlToo7i64DSXfn
         jG4j1LWx76IlwkU7GQXrrUHOjyOaSUk83PgvXvKHsvVYGob+TmjsbxruT/pTu/wBnhqR
         ew8PsygtILx2gfT8GWI0ObM1GWqFxmghszIyzDO/cQxKpoOYptICthxpSuao6EDjItNh
         vi0Q==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=from:mime-version:sender:precedence:list-unsubscribe:subject
         :message-id:feedback-id:to:date:dkim-signature;
        bh=Btp8oSgJ9w+IbGn74ULnX74LZxjlwZ68I1gz/FbCWkU=;
```

Fig.73. Análisis de la cabecera de un correo electrónico.

Por otra parte, cada uno de estos saltos al igual que los casos anteriores, nos proporciona las direcciones IP y MAC de los saltos que este hizo, por lo tanto, es conveniente analizar el primero para conocer la posible ubicación del delincuente. Como resultado del intento de encontrar la dirección es que el atacante realizó el acto ilícito desde los Estados Unidos.

IP address	**209.85.202.101** (change)
Latitude	37.751
Longitude	-97.822
Country	United States
Region	
City	
Organization	Google Servers

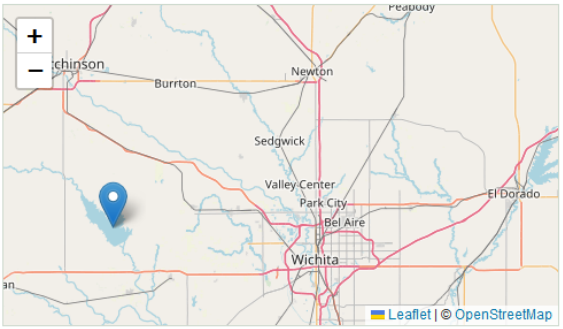


Fig.74. Posible dirección del atacante

A continuación, se muestra el uso de otra herramienta para análisis de cabeceras de correos electrónicos en donde muestra la información resumida de la cabecera de una manera más detallada para el análisis a realizar. Se puede apreciar el número de saltos dado por el mensaje de correo electrónico junto con direcciones MAC, hora y fecho de los dispositivos que recibieron y enviaron el correo electrónico tipo phishing. Mediante esta información se sigue los pasos que realizó el correo electrónico hasta llegar a su destino.

Summary

Received headers

Hop↓	Submitting host	Receiving host	Time	Delay	Type ⇒
1	o64.email.sendgrid.com(unknown)	ismtpd0083p1sjc2.sendgrid.com (SG)	1/12/2023 10:52:33 AM		ESMTP
2		filter9856p1mdw1.sendgrid.com	Invalid Date		SMTP
3	2hqd.topflightstairliftsuk.co.uk ([2a01:7e01::f03c:93ff:fe51:12ba])	smtp-relay.gmail.com	1/12/2023 10:54:16 AM	1 minute 43 seconds	ESMTPS
4	mail-sor-f101.google.com (mail-sor-f101.google.com. [209.85.220.101])	mx.google.com	1/12/2023 10:54:16 AM	0 seconds	SMTPS
5		2002:ac4:9303:0:b0:58a:95f4:7b15	1/12/2023 10:54:17 AM	1 second	SMTP

Fig.75. Análisis realizado por Message Header Analyzer Azure Caso 5

Cuerpo

En el cuerpo de este correo electrónico se puede encontrar una imagen perteneciente a un anuncio que puede llamar la atención de la víctima, para este caso específico están

ofreciendo un seguro de autos afirmando que es el más económico que pueden encontrar en el mercado.

En el análisis del cuerpo del mensaje se encuentran otros mensajes que no fueron visualizados por la víctima, estos mensajes ocultos también corresponden a ofertas de cursos de fotografías, verificación de correo electrónico, supuesta confirmación de cuentas además de subscripciones a servicios no requeridos por la persona que recibe el email.

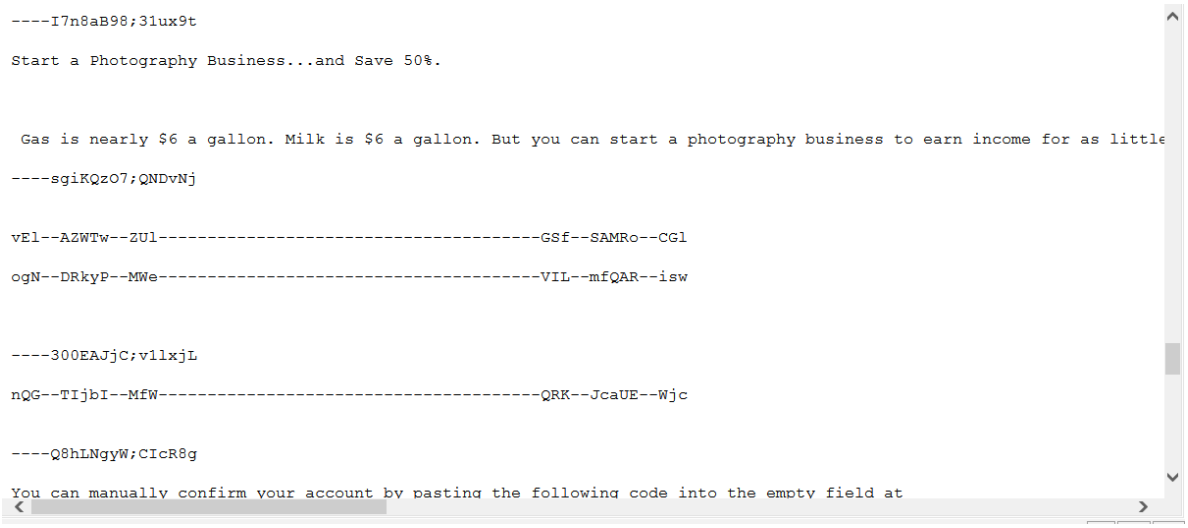


Fig.76. Posible esteganografía en el Caso 5

Anexo 9

En el presente Anexo se detalla todo el proceso por fases del experimento 6 (Correo electrónico Malware).

FASE DE ADQUISICIÓN

En este correo electrónico se adjunta un mensaje de correo electrónico con asunto de confirmación de pago, en donde en el cuerpo del mensaje posee un texto afirmando que el envío de un dinero fue éxitos y que se necesita de una firma, es aquí en donde el atacante adjunta un supuesto comprobante de la transacción realizada.

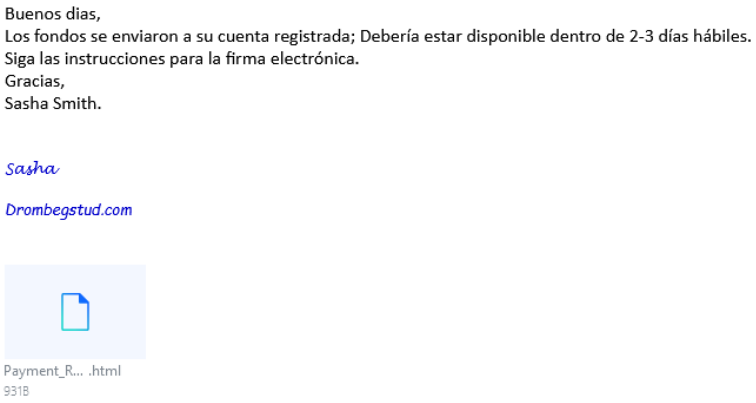


Fig.77. Correo electrónico malware

Mediante un análisis previo al documento con la herramienta de Virus Total en documento que lleva el nombre “Payment_Receipt_.html”, no posee rastros de estar infectado, sin embargo, es necesario realizar un análisis más profundo para encontrar los resultados esperados.

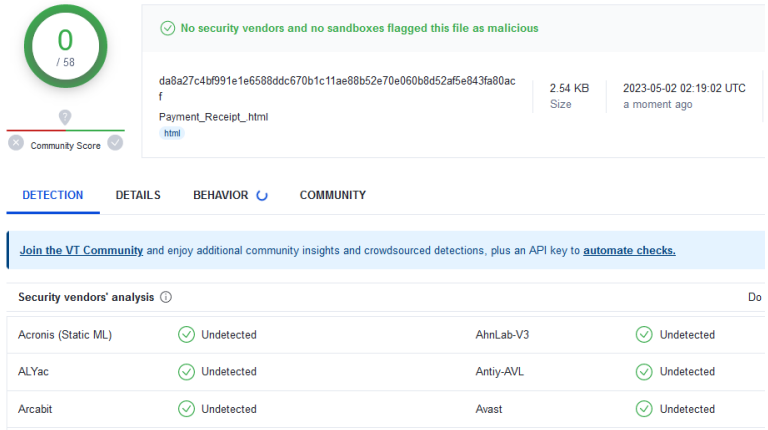


Fig.78. Análisis con Virus Total

FASE DE PRESERVACIÓN

En la presente fase el objetivo es adquirir el código hash codificado en SHA1 del presente experimento utilizando QFileHasher, obteniendo como resultado los siguientes caracteres pertenecientes al archivo en cuestión: **dfc4592df5b5d0a85f888b0426ba4ee2676a86e0.**

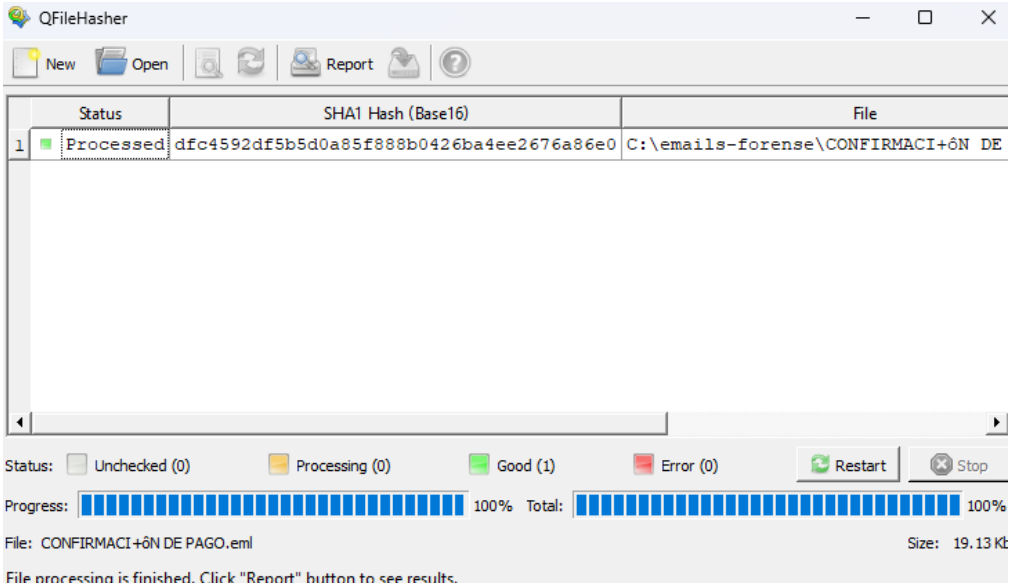


Fig.79. Código hash para caso 6

FASE DE ANÁLISIS

Cabecera

A continuación, se muestra el uso de otra herramienta para análisis de cabeceras de correos electrónicos en donde muestra la información resumida de la cabecera de una manera más detallada para el análisis a realizar. Se puede apreciar el número de saltos dado por el mensaje de correo electrónico junto con direcciones MAC, hora y fecho de los dispositivos que recibieron y enviaron el correo electrónico con malware. Mediante esta información se sigue los pasos que realizó el correo electrónico hasta llegar a su destino.

```
Received: from DM6PR06MB6298.namprd06.prod.outlook.com (::1) by
 PH0PR06MB7189.namprd06.prod.outlook.com with HTTPS; Fri, 25 Nov 2022 22:44:59
 +0000
Received: from BY3PR10CA0014.namprd10.prod.outlook.com (2603:10b6:a03:255::19)
 by DM6PR06MB6298.namprd06.prod.outlook.com (2603:10b6:5:12d::20) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5857.17; Fri, 25 Nov
 2022 22:44:58 +0000
Received: from SJ0PR03MB5903.namprd03.prod.outlook.com
 (2603:10b6:a03:255:cafe::a2) by BY3PR10CA0014.outlook.office365.com
 (2603:10b6:a03:255::19) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5857.20 via Frontend
 Transport; Fri, 25 Nov 2022 22:44:58 +0000
ARC-Seal: i=2; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv=pass;
 b=W3TE9zpCPCd0nNhC18c3BlnTGnKl2rOX124f3XSETtaWZux4zbuMPa+C1WI6d1DOidiZNApsFLpP3
ARC-Message-Signature: i=2; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com;
 s=arcselector9901;
```

Fig.79. Análisis de la cabecera Caso 6

Por otra parte, cada uno de estos saltos al igual que los casos anteriores, nos proporciona las direcciones IP y MAC de los saltos que este hizo, por lo tanto, es conveniente analizar el primero para conocer la posible ubicación del delincuente. Como resultado del intento de encontrar la dirección es que el atacante realizó la actividad ilícita desde Los Estados Unidos, Virginia.

IP address	**40.92.20.10** (change)
Latitude	36.6534
Longitude	-78.375
Country	United States
Region	Virginia
City	Boydton
Organization	Microsoft Azure

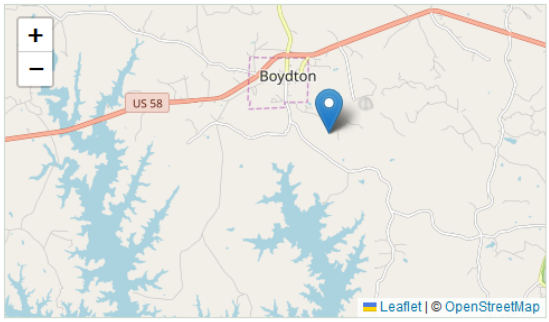
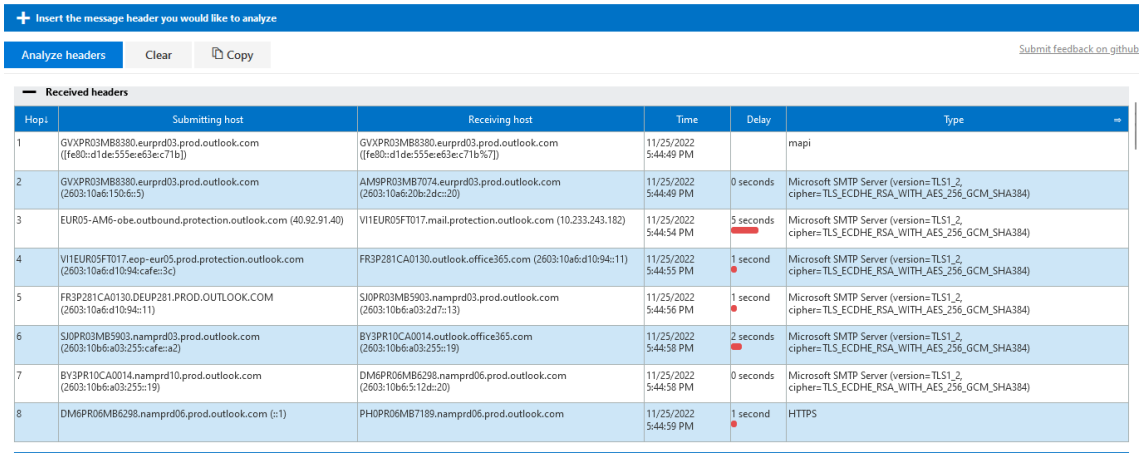


Fig.80. Posible ubicación del ciberdelincuente Caso 6

A continuación, se muestra el uso de otra herramienta para análisis de cabeceras de correos electrónicos en donde muestra la información resumida de la cabecera de una manera más detallada para el análisis a realizar. Se puede apreciar el número de saltos dado por el mensaje de correo electrónico junto con direcciones MAC, hora y fecha de los dispositivos que recibieron y enviaron el correo electrónico tipo malware. Mediante esta información se sigue los pasos que realizó el correo electrónico hasta llegar a su destino.



Hop↓	Submitting host	Receiving host	Time	Delay	Type
1	GVXPR03MB8380.eurprd03.prod.outlook.com ([fe80::d1de:555e:e63e:c71b])	GVXPR03MB8380.eurprd03.prod.outlook.com ([fe80::d1de:555e:e63e:c71b%7])	11/25/2022 5:44:49 PM		mapi
2	GVXPR03MB8380.eurprd03.prod.outlook.com (2603:10a6:150:6::5)	AM9PR03MB7074.eurprd03.prod.outlook.com (2603:10a6:20b:2dc::20)	11/25/2022 5:44:49 PM	0 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
3	EUR05-AM6-obe.outbound.protection.outlook.com (40.92.91.40)	VI1EUR05FT017.mail.protection.outlook.com (10.233.243.182)	11/25/2022 5:44:54 PM	5 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
4	VI1EUR05FT017.eop-eur05.prod.protection.outlook.com (2603:10a6:d10:94:cafe::3c)	FR3P281CA0130.outlook.office365.com (2603:10a6:d10:94::11)	11/25/2022 5:44:55 PM	1 second	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
5	FR3P281CA0130.DEUP281.PROD.OUTLOOK.COM (2603:10a6:d10:94::11)	SJ0PR03MB5903.namprd03.prod.outlook.com (2603:10b6:a03:2d7::13)	11/25/2022 5:44:56 PM	1 second	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
6	SJ0PR03MB5903.namprd03.prod.outlook.com (2603:10b6:a03:255:cafe::a2)	BY3PR10CA0014.outlook.office365.com (2603:10b6:a03:255::19)	11/25/2022 5:44:58 PM	2 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
7	BY3PR10CA0014.namprd10.prod.outlook.com (2603:10b6:a03:255::19)	DM6PR06MB6298.namprd06.prod.outlook.com (2603:10b6:5:12d::20)	11/25/2022 5:44:58 PM	0 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
8	DM6PR06MB6298.namprd06.prod.outlook.com (::1)	PH0PR06MB7189.namprd06.prod.outlook.com	11/25/2022 5:44:59 PM	1 second	HTTPS

Fig.81. Análisis realizado por Message Header Analyzer Azure Caso 6

Anexo 10

FORMATO DE INFORME PERICIAL

El presente informe consta con información obtenida a través del uso de las herramientas de informática forense usadas en las diferentes fases ya realizadas para cada uno de los casos tratados en este proyecto: Phishing, Malware Troyano, Estafa, Apropiación de cuentas y Malware. Tomando los debidos cuidados y proceso para preservar la información adquirida y la máquina física que realizará el procedimiento de análisis.

El proceso de investigación se rige mediante el estándar UNE 71506:2013 constando de 4 fases: Adquisición, preservación, análisis y documentación. Utilizando herramientas de análisis forense se analizará lo que está estipulado en el punto anterior, aplicando conocimiento en generación de código hash para verificar la autenticidad de esta información, análisis de encabezados, identificación de huellas digitales y rastros de los posibles atacantes relacionados con cada uno de los casos seleccionados en el punto anterior.

Después del análisis realizado a los archivos adquiridos y preservados se emiten las siguientes conclusiones recalcando que lo más importante de él análisis de correos electrónicos es las huellas digitales del delincuente que en este caso es: correo electrónico y direcciones IP.

Caso 1. Apropiación de cuentas o correo Zombie

Después del análisis realizado a este tipo de correo cabe recalcar que se encuentran 2 tipos de huellas digitales que pueden dar con la pista del posible delincuente, el primero es la dirección del correo electrónico en este caso el correo electrónico que fue el emisor del mensaje es rectorado@upse.edu.ec por lo que se presume que usaron esta dirección de email para replicar el correo electrónico malicioso.

Por otra parte, las diferentes direcciones IP son saltos realizados por el mensaje electrónico enviado, se presume que la primera IP encontrada como "**10.173.99.22**" es la dirección IP del presunto delincuente debido a que fue ahí donde salió el correo electrónico.

Caso 2. Correo electrónico Phishing

Se requiere aprovechar de las huellas digitales de la persona en cuestión para encontrar al posible responsable, mediante la dirección IP proporcionada por la cabecera, se puede realizar un pequeño análisis como la anterior expuesta para obtener su posible ubicación además del correo electrónico asociado con este tipo de ataca a un mensaje electrónico. Como resultado del análisis se obtiene que el correo electrónico involucrado es yolissa-4@hotmail.com además se encuentra camuflado para que el usuario vea la siguiente dirección "banco@pichincha.com ..."y como dirección IP involucrada está la siguiente: 10.13.6.249.

Caso 3. Correo electrónico con Estafa o Engaños

Para este caso específico se puede encontrar relacionado 2 direcciones de correos electrónicos como sospechosos debido a que no pertenecen al receptor de la información en este caso victoria.haz@hotmail.com, sin embargo, los siguientes: espagnoljudicialpolicia@gmail.com y yeoissa2019@hotmail.com son los implicados como sospechosos analizando la cabecera se puede observar diferentes saltos, cada uno de estos al igual que los casos anteriores, proporciona las direcciones IP y MAC.

Caso 4. Correo electrónico Malware (Troyano)

Para este caso se puede encontrar la dirección IP que envió el correo electrónico malicioso, la IP es **190.15.141.157,** el mensaje electrónico dio un total de 7 saltos visibles hasta poder llegar a su destino. Dentro del cuerpo del correo electrónico se puede observar un archivo adjunto, que mediante el análisis se determina que el archivo posee malware de tipo troyano.

Caso 5. Correo electrónico con Ingeniería Social

El correo electrónico relacionado para este caso es el siguiente renzonqc@gmail.com este correo electrónico le pertenece a la víctima, sin embargo, asegura no haber enviado información como esa, por otra parte, la dirección IP encontrada es **209.85.220.101**, presumiblemente sea la dirección IP de la persona que realizó el ataque, en el análisis de su estructura se puede encontrar información camuflada por lo que también se considera que posee esteganografía.

Caso 6. Correo electrónico con Malware

Mediante el análisis realizado para este caso se puede determinar que el correo electrónico u_reina2@hotmail.com está relacionado con el ataque así mismo como la dirección IP de emisión del mensaje **10.152.24.234,** en parte de la estructura del mensaje se puede encontrar un documento adjunto de tipo html dentro del mensaje.