DATA LEAKAGE CASE PART I

JUAN CARLOS PRADA MARIN
OSCAR NIETO RAMOS
AUTORES

UNIVERSIDAD PILOTO DE COLOMBIA
SECCIONAL DEL ALTO MAGDALENA
FACULTAD DE INGENIERÍA
PROGRAMA SISTEMAS
GIRARDOT
2022

DATA LEAKAGE CASE PART I

JUAN CARLOS PRADA MARIN
OSCAR NIETO RAMOS
AUTORES

ELECTIVA OPCION DE GRADO

EDICSON PINEDA
Ingeniero de Sistemas

UNIVERSIDAD PILOTO DE COLOMBIA
SECCIONAL DEL ALTO MAGDALENA
FACULTAD DE INGENIERÍA
PROGRAMA SISTEMAS
GIRARDOT
2022

Tabla de Contenido

Lista de Figuras

Lista de tablas

1. Resumen

La presente investigación hace referencia a la fuga de datos, que se dio en una empresa internacional dedicada a desarrollar tecnologías y dispositivos de última generación, en la que se encontraron muchas falencias en cuanto a la seguridad de la información: Confidencialidad, integridad y disponibilidad de los datos. En el análisis forense digital se llevaron a cabo 5 fases técnicas para extraer información: Adquisición, Preservación, Análisis de la evidencia, Documentación y Presentación de resultados, las cuales permitieron demostrar los incidentes que se ocasionaron dentro de la empresa en la que trabajaba Iaman. Para dicha recolección de pruebas se utilizó Autopsy, una herramienta antiforence que analiza imágenes, archivos, documentos que son modificados y eliminados en el disco de almacenamiento de un computador en cierto tiempo.
Palabras claves: Autopsy, análisis, fuga, delitos, seguridad, datos, forense.

Abstract

The present investigation refers to the data leak, which occurred in an international company dedicated to developing state-of-the-art technologies and devices, in which many shortcomings were found in terms of information security: Confidentiality, integrity and availability of the data. In the digital forensic analysis, 5 technical phases were carried out to extract information: Acquisition, Preservation, Evidence Analysis, Documentation and Presentation of results, which allowed demonstrating the incidents that occurred within the company where Iaman worked. For this collection of evidence, Autopsy was used, an anti-forence tool that analyzes images, files, documents that are modified and deleted on a computer's storage disk at a certain time.
Keywords: Autopsy, analysis, escape, crimes, security, data, forensic.

2. Introducción

La presente investigación hace referencia a un joven llamado Iaman, el cual trabajaba como gerente de la división de una famosa empresa internacional, dedicada a desarrollar tecnologías y dispositivos de última generación. Gracias a su codicia cometió delitos informáticos, filtrando información privada de su empresa a Spy, un agente externo el cual le prometía grandes sumas de dinero a cambio de mantenerlo informado y enviarle muestras confidenciales, esta fuga de datos se hizo a través de:

a) Almacenamiento en la nube personal
b) Servicio de correos electrónicos para establecer relación comercial
c) Memoria USB Y CD
d) Computador personal

El informante es descubierto por el control de seguridad de la empresa cuando inicia a copiar los archivos en sus dispositivos de almacenamiento, en causa que el espía solicito la entrega de los datos restantes de esa forma. Inmediatamente se procede a realizar la verificación si hubo fuga de datos a través de sus dispositivos, pero al finalizar no se encontró nada. Sin embargo, Iaman violó las políticas de la empresa portando elementos no autorizados, accediendo a documentos confidenciales fuera del rango de tiempo establecido, utilizando otros usuarios y permisos, por lo que se procedió llevar el caso al laboratorio de análisis forense digital para su respectivo análisis.
Según el DFRWS (taller de investigación digital forense) La informática forense consiste en el empleo de métodos científicos comprobables para preservar, recolectar, validar, identificar, analizar, interpretar, documentar y presentar evidencias digitales procedentes de fuentes digitales con el propósito de hacer posible la reconstrucción de hechos considerados delictivos. (CONFERENCE, 2001).
Esto se hace con el objetivo de agrupar y extraer información de cualquier dispositivo tecnológico que se utilizó para cometer el ataque o delito informático con el fin de encontrar la evidencia original de este.

3. Justificación

Este documento se centra en la investigación de un caso de fugas en una empresa, esta fuga de datos fue causada por un trabajador de la empresa, el cual con la computadora de escritorio que se le es brindada en la empresa comienza a almacenar y enviar información sobre proyectos secretos que se están realizando, con esta información se plantea analizar los dispositivos de almacenamiento que fueron utilizados por el trabajador para recabar pruebas suficientes y demostrar los actos delictivos.

Gracias a casos como estos se puede estudiar la manera y conducta de personas que desean realizar delitos utilizando dispositivos informáticos, con ello se pueden estudiar las diferentes posibilidades que la información puede ser tratada y modificado en este tipo de casos, debido a que suceden en múltiples ocasiones actos delictivos con orígenes similares es necesario realizar un estudio demostrando cómo las diferentes herramientas forenses brindan ayuda necesaria para revelar y demostrar de manera precisa los suceso de los acontecimientos

4. Objetivos

Objetivo General

Estudiar el caso de la fuga de datos que se presento en una organización donde se desarrollaban tecnologías de ultima generación, ofreciendo un análisis y línea de tiempo detallado, sobre cómo sucedieron los acontecimientos y quienes fueros los implicados.

Objetivos Específicos

Analizar el dispositivo de almacenamiento del computador

Proveer evidencias utilizando el software forense Autopsy

Crear tablas de las diferentes particiones relevantes al caso

Explicar y demostrar las faltas graves y delitos causadas por el trabajador

5. Marco Teórico

5.1 Delito Informático

Se representa como todo acto mediante el uso de algún elemento informático que atente contra los derechos de otra persona o usuario de herramientas tecnológicas, mediante la utilización de hardware o software.

5.2 Naturaleza Juridicial

El usuario o el afectado tendrán a toda disposición la oportunidad de ser protegido y mantenerse en una relación en donde le permita mantener el control y orden social después del ataque.

5.3 Tipos de delitos informáticos

Existen diferentes maneras en las que personas usuarias puedan ser atacadas o se les pueda vulnerar su seguridad mediante herramientas tecnológicas en algunos casos los usuarios son víctimas de robo de información y violación de datos personales.

5.4 Informática forense

La informática forense definida según el DFRWS (taller de investigación digital forense) consiste en el empleo de métodos científicos comprobables para preservar, recolectar, validar, identificar, analizar, interpretar, documentar y presentar evidencias digitales procedentes de fuentes digitales con el propósito de hacer posible la reconstrucción de hechos considerados delictivos. (CONFERENCE, 2001)

Es un campo de la investigación en donde se utilizan principios de la investigación científica, para la realización de análisis profundos a sistemas operativos o herramientas tecnológicas con la finalidad de obtener evidencias de un incidente.

5.5 Objetivos de la informática forense

Una de las mayores tareas de la informática forense es realizar un estudio de los métodos utilizados para vulnerar la seguridad de los usuarios, de esta manera se podrán crear planes de contra medidas y nuevas estrategias para protegerlos

El siguiente objetivo es la agrupación y extracción de cualquier dato que estuvo implicado en un ataque o delito informático con el fin de encontrar el origen o proceso de este.

5.6 Alcance de la informática forense

Las virtudes que ofrece la informática forense son valiosas para la investigación de incidentes relaciones con herramientas tecnológicas, debido a que gracias a las bases y principios toda la información relacionada con el caso estará preparada y lista cuando se deba realizar un motivo de investigación y se lleve a un caso o juicio extenso.

5.7 Usos de la informática forense

La informática forense es un proceso valioso que intenta ayudar a los usuarios si son vulnerados, usualmente los forenses informáticos trabajan para empresas las cuales son las mayores víctimas de fraudes informáticos o ataques, para estos casos las empresas importantes tienen siempre listo un equipo de profesionales experto en el manejo y contramedida de este tipo de inconvenientes que se suelen dar.

5.8 Retos de la informática Forense

Con el pasar del tiempo las sociedad y las herramientas que utilizan se adaptan y evolucionan esto no es un misterio, en los tiempos en los que se vive actualmente existen múltiples dispositivos y aplicaciones que nos facilitan la vida en nuestro día a día pero algunas personas utilizan estas herramientas de manera indebida con el objetivo de vulnerar y atacar la seguridad de otras personas con este reto en mente los forenses informáticos deben adaptarse igualmente preparándose para cualquiera nuevo tipo de ataque y aprender de los anteriores con el fin de garantizar seguridad a todos los usuarios.

5.9 Ingeniería Social

Según Avast & Kaspersky lo definen como un conjunto de técnicas que se usan para engañar y manipular a las personas u usuarios con el fin de violar la seguridad de los sistemas de información, para tener acceso a información confidencial, robar datos, dinero u otros bienes materiales. Para que los ataques sean exitosos debe existir una vulnerabilidad de software.

El ingeniero social realiza esta técnica para obtener la información de las personas sin que se dé cuenta que ha sido una víctima de un delito informático. (Flórez & Méndez, 2017, p.26)

Según (Ramos, 2015) en el libro de Hacking con Ingeniería social, técnicas para hackear humanos, refiere que el arte de la ingeniería social tiene como objetivo principal hackear seres humanos, es decir conseguir que hagan algo de forma voluntaria que de otra forma no harían y que beneficie al atacante. (p.17)

La ingeniería social es practicada por los piratas informáticos y hackers para tener acceso a los sistemas de información y así robar y delinquir cibernéticamente cada una de las pertenencias económicas de una entidad u organización, muchos de estos factores son un enemigo muy fuerte que actualmente se sigue luchando con técnicas y métodos nuevos para que de esta manera las empresas no fracasen.

5.10 Fuga de Información

¿Cuál es la importancia que se le da a la fuga de información en una BD?

Según la revista La Nación de Santiago de Chile permite conocer la fuga de información como una realidad que afecta tanto a empresas como a usuarios finales y aunque el fin último y la proporción de los daños pueden variar, la constante es que las víctimas siempre resultan afectadas y vulneradas en su privacidad. Los registros muestran que a nivel mundial en los últimos años la fuga de datos ha ido en constante aumento.

Los principales riesgos externos de la pérdida de datos: Malware, Ataques vía e-mail, phishing, entre otros. Todos ellos tienen como blanco extraer información crítica y sensible para la empresa, ya sea financiera, estratégica, confidencial, entre otras, lo que puede desembocar en incalculables pérdidas de ingresos, grave daño a la reputación de la compañía y gran deterioro a la confianza de los clientes.

Teniendo en cuenta toda esta información nos permite conocer las debilidades de los sistemas de información, los accesos no autorizados a la información confidencial y así diseñar en la base de datos los diferentes roles de los usuarios y crear restricciones.

Las vulnerabilidades en la seguridad de la información o de los datos es un factor de riesgo que puede acabar con la economía de una empresa u organización, puede producirse tanto en países desarrollados como en países subdesarrollados, por ente se presentan muchos casos de suplantación de datos, amenazas, ataques cibernéticos y robos de información en beneficios a

terceras personas, casos de estos se presentaron en algunos países de Estados Unidos que a continuación se relacionan.

Según la Revista Reforma del texto Lidera México en ciberataques publicado el 7 de octubre del 2013, en la Agencia de Seguridad Nacional de los Estados Unidos (NSA) se presentó un gran incidente de fuga de información en los informes militares, debido a este robo de información EEUU se ha enfrentado a numerosas críticas de otros países y organizaciones de derechos civiles.(Guerrero,2013).

Este tipo de delitos pueden causar grandes pérdidas financieras o dañar gravemente la reputación de una empresa u organización. Según los acontecimientos presentan a México como el país más vulnerable a estos ataques.

Según Guevara, Cesar en su tesis doctoral "Desarrollo de Algoritmos eficientes para identificación de usuarios en accesos informáticos" plantea que los ciberataques son un problema de mayor importancia en organizaciones empresas e instituciones. En las últimas décadas las redes han crecido de manera exponencialmente debido al gran número de computadores, servidores y equipos. Debido al acceso tan abierto a los datos, ya que la información es uno de los activos más importantes de las empresas y negocios. Los ciberataques son un problema de gran envergadura que afecta a la mayoría de las personas y empresas alrededor del mundo. Este problema se puede describir como la transmisión o manipulación de datos privados de forma no permitida desde una organización a un agente externo (persona u organización no autorizada). En la actualidad es un problema realmente preocupante y una amenaza a la seguridad. Los datos confidenciales de instituciones y personas incluyen propiedad intelectual, información financiera, información de carácter personal y gran variedad de contenidos en función de los negocios y las industrias involucradas. (Guevara, 2017, pág. 19)

Un reciente estudio presentado por McAfee, compañía de software especializado en seguridad informática, reveló que Colombia presenta serios problemas en esta área (El Espectador, 2014). Según Juan Pablo Páez gerente de preventa de McAfee, el problema de temas de seguridad de datos con mayor frecuencia se presentan en el área de telecomunicaciones y financiero, puede llegar a altos niveles de pérdidas o crisis financiera.

El reporte de amenazas de McAfee Lab, deja ver, además, que cada trimestre 100.000 nuevos computadores se adhieren a la red de atacantes, y que sólo se puede combatir entendiendo que la seguridad es la base de los negocios y del país y reforzando la formación básica de profesionales.

También mostró que las organizaciones débiles en este tema lo son porque: "En Colombia hay un modo reacción, hasta que no pasen las cosas no se toman decisiones, y porque no han liderado esquemas que obliguen a cumplir con este requisito".

El pharming es uno de los principales delitos informáticos que se presentan en nuestro país que utilizan personas inescrupulosas llamadas hackers para obtener beneficios económicos e información privilegiada. Este tipo de ataque busca la obtención de la información bancaria, credenciales de acceso e información personal, esto ocurre cuando se ingresa a la dirección de una página web insegura, maliciosa y desconocida, debido a la vulnerabilidad de la falsificación de URL en Internet Explorer, permite crear páginas maliciosas para engañar a sus usuarios.

Los correos infectados es una de las técnicas favoritas que presentan los ciberdelincuentes para atacar a sus víctimas (Empresas u Organizaciones) ya que la necesidad de hacer uso de un correo electrónico es permanente, bien sea para enviar información o establecer comunicación con otras personas de su interés. Según Jaime Monsalve experto en el tema, expone en su artículo Ciberseguridad: Principales Amenazas en Colombia (Ingeniería Social, Phishing y Dos, de acuerdo con los estudios realizados por la página web Infospyware, un atacante puede ganar 10.000 USD. La técnica consiste en enviar un ataque 1.000.000 correos maliciosos, de los cuales 5.000 los usuarios con desconocimiento ingresan a esas páginas y finalmente 1000 usuarios diligencian los datos solicitados. Esta técnica o ataque cibernético permite que cada vez las empresas estén en amenaza y que su actividad financiera esté involucrada y hasta puede llegar a acabar con la imagen.

¿En este caso que se puede hacer para proteger las empresas?

El phishing es un ataque cibernético que incrementa exponencialmente debido al desconocimiento de las personas y a la baja seguridad de los sistemas de información, para poder mitigar estos ataques, es necesario realizar capacitaciones en temas de ciberseguridad para que los usuarios incrementen más su conocimiento y las empresas que se vean afectadas inviertan más en seguridad cibernética y las que no se mantengan sólidas ante estos ataques. (Monsalve, 2018, pág. 5)

DOS y DDOS son ataques a la red que deniega los servicios, para que tanto los usuarios y la organización no puedan acceder a cada recurso, por lo cual son considerados las amenazas más peligrosas y potentes que utilizan los hackers para atacar los servidores.

¿Qué técnicas se pueden utilizar frente a estas amenazas?

Utilizando estenografía y criptografía en el desarrollo de los sistemas de información. Estas técnicas se llevan a cabo mediante un proceso de encriptación que protegen de manera segura y estable cada contraseña e información privilegiada de una empresa u organización.

5.11 Implementation Methodology of a Quality Management System in a Digital Forensic Laboratory.

Este laboratorio se desarrolló en Argentina, en la universidad Mar de Plata, por el Grupo de Investigación y Extensión Mejora Continua y Medio Ambiente, conformados por: Ambrústolo, Mariela B., Lorio, Ana H., Cistoldi, Pablo., Greco, Fernando., Trigo, Santiago., Migueles, Marina., Bruno, Constanzo., & Giordano, Roberto. (2020).

Consistía en un Sistema de Gestión de Calidad para laboratorios de análisis forenses, su objetivo prcipal se basaba en crear una guía respecto a la realización de laboratorios de informática forense. Para su desarrollo, tuvieron en cuenta ocho tareas, las cuales se dividieron en cinco etapas:

- Diseño:
  Instrumentos e instancias formales para la eleboración de una guía técnica de implementación.
- Mapeo:
  Integración de los procesos y procedimientos del SGC.
- Herramientas:
  Diseño, mapeo, e integración de los procedimientos y registros
- Aplicación:
  Pruebas y validaciones de la guía una implementación de un SGC
- Ajuste:
  Guía y SGC, elaboración de las conclusiones e informe final del proyecto.

El uso de estas 5 etapas de este laboratorio fue de gran importancia para el desarrollo del caso de fuga de datos, ya que se utilizaron herrramientas para llevar a cabo un mapeo y seguimiento de los datos. Se llevo a cabo un diseño para la elaboración de un informe técnico, mediante la recoleccion de información de distintas fuentes para el análisis y presentación de resultados que estipulan los aptos de violacion de políticas y delitos informáticos.

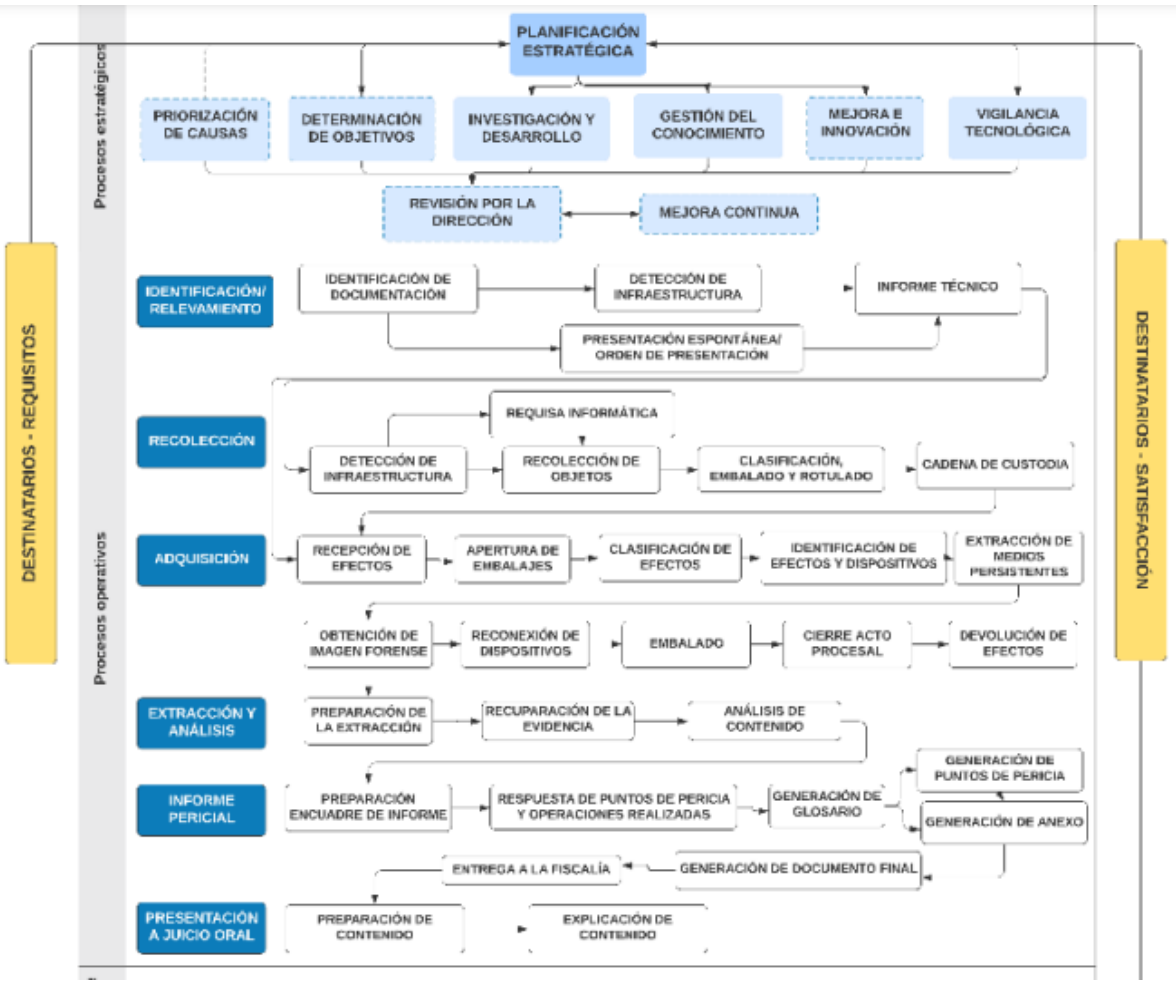


Fig 1. Mapeo de Procesos del LIF Mar de Plata
Fuente: Universidad Fasta, Argentina

Este mapa de procesos permitió llevar a cabo un orden al recolectar la información, los pasos que se deben seguir en cada situación, para hacer buen uso de los datos y el análisi forense digital de las evidencias, para obtener mejores resultados en la investigación del caso.

Fig. 2. Matriz FODA
Fuente: Elaboracion propia

La matriz FODA permite gestionar en un laboratorio de informática forense, los aspectos positivos del entorno exterior y su proyección futura, aspectos negativos da la situación interna actual, aspectos positivos de una situación interna actual y aspectos negativos del entorno exterior y su proyección futura. Esto con el fin de corregir falencias e implementar mejoras para uno mejor proyección.

.

5.12 Fases fundamentales del análisis forense digital

De acuerdo con lo planteado, por la empresa ESET NOD32 ANTIVIRUS, en su documento redactado el 15 de abril de 2015, se llevan a cabo 5 fases que son fundamentales para todo análisis forense digital, las cuales ayudan a mantener un estudio estructurado.

1. Adquisición

Se obtienen copias realizando copias de bite a bite, obteniendo como resultado una imagen de igual tamaño, para esto la evidencia se debe rotular con fecha y hora que fue recaudada, mantener en un lugar seguro para que no entre en contacto con el medio. Se recomienda utilizar guante, bolsas antiestáticas y jaulas de Faraday para depositar dispositivos que puedan interaccionar con ondas electromagnéticas

2. Preservación

La preservación documental consiste en garantizar que los documentos, registros y archivos informáticos de la organización mantengan siempre su total confiabilidad. Este concepto varía de acuerdo con distintos autores, a los contextos documentales y al tipo de organización a la que la información esté asociada. En un contexto archivístico y en donde tratamos de operar un enfoque de seguridad informática con uno de preservación digital. (Voutssas, 2010).

En esta etapa se debe garantizar la información recopilada con el fin de que no se destruya o sea transformada la evidencia original. Es decir que nunca debe realizarse un análisis sobre la muestra incautada, para esto se debe realizar una copia de la evidencia, para luego realizar el análisis forense que permita llevar dicha pericia.

3. Análisis de la evidencia

Una vez obtenida la información y preservada, se continúa con la fase técnica, donde se utilizan hardware y software para hacer el análisis forense. Existen diferentes tipos de herramientas para llevar a cabo este proceso:

- Autopsy
- Caine
- Digital Forensics Framework
- Volatilidad

- Redline
- Cofee
- Wreshark
- DumpZilla
- Estación de trabajo Sift
- Exiftool
- Bul Extractor
- Ftk Imager

Todas estas herramientas permiten hacer un análisis exhaustivo, teniendo en cuenta las capacidades y experiencia del analista para dar mejores resultados frente al incidente.

4. Documentación

En esta etapa final, la documentación es muy importante, ya que en ella se recopilan todos los datos y acontecimientos del incidente, también se debe establecer una relación lógica de las pruebas obtenidas

5. Presentación de resultados

Para dar cumplimiento a esta etapa, se redacta un informe ejecutivo que reúna lo más pertinente e importante del objeto de la investigación, debe redactarse en lenguaje natural, ser muy claro, preciso y conciso, para no generar ninguna duda.

Por otra parte se realiza un segundo informe llamado Informe técnico, se centra en las técnicas y resultados, que es el de mayor grado para finalizar la investigación.

Esta fue la metodología que se utilizó para llevar a cabo el caso de la fuga de datos que se presentó en la investigación, donde se utilizó como principal herramienta de trabajo un computador para instalar en programa de análisis forense Autopsy y Ftk Imager, el cual permitió incautar, imágenes, copias de proyectos y otros archivos que mostrarán los indicios del incidente. Obteniendo como resultado archivos borrados de Iaman, conversaciones comprometedoras entre Iamant y Spy, utilizando como principal medio correos para establecer vínculos personales donde cedía información privilegiada de su empresa por un monto de dinero

6. Marco Conceptual

6.1 Sabotaje Informático

El delito de daño informático, también llamado sabotaje informático, hace referencia a conductas de destrucción, supresión, deterioro, alteración, menoscabo, o de actos tendientes a impedir el acceso; las que deben recaer sobre un objeto material específico, en este caso, la totalidad o parcialidades del soporte lógico (software) de un computador (Herrera, 2018)

6.2 Laboratorio de informática forense

Establecimiento en donde se llevan a cabo tareas de investigación de evidencias en donde se utilizan herramientas de hardware y software como dispositivos de captura de imágenes, estaciones de recuperación de datos y creadores de copias de seguridad.

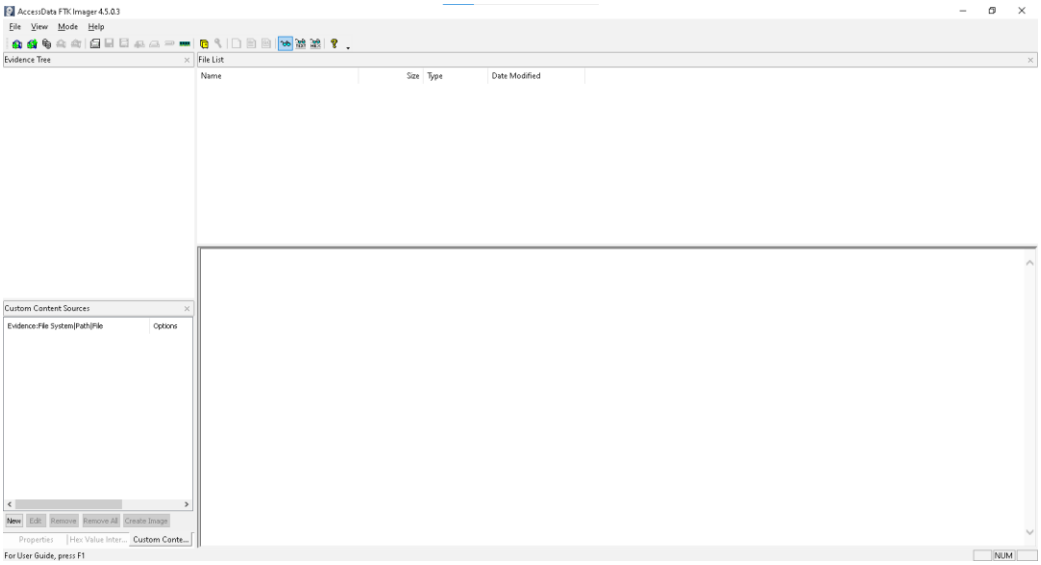
Según (integral, 2019) “Conozca esta innovadora solución tecnológica para la gestión de incidentes informáticos, a través de un conjunto de dispositivos y aplicaciones especializadas que permiten adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional para que sean válidos dentro de un proceso legal o de una investigación.

6.3 FTK Imager

Aplicación de análisis de evidencia digital para datos e imágenes utilizada para la verificación previa antes de continuar con un análisis avanzado de los datos.

Según (Insectra, 2021) “es una herramienta de imágenes y vista previa de datos que le permite evaluar rápidamente la evidencia electrónica para determinar si se justifica un análisis adicional con una herramienta forense como Forensic Toolkit.

Ilustración 1 interfaz de FTK Imager



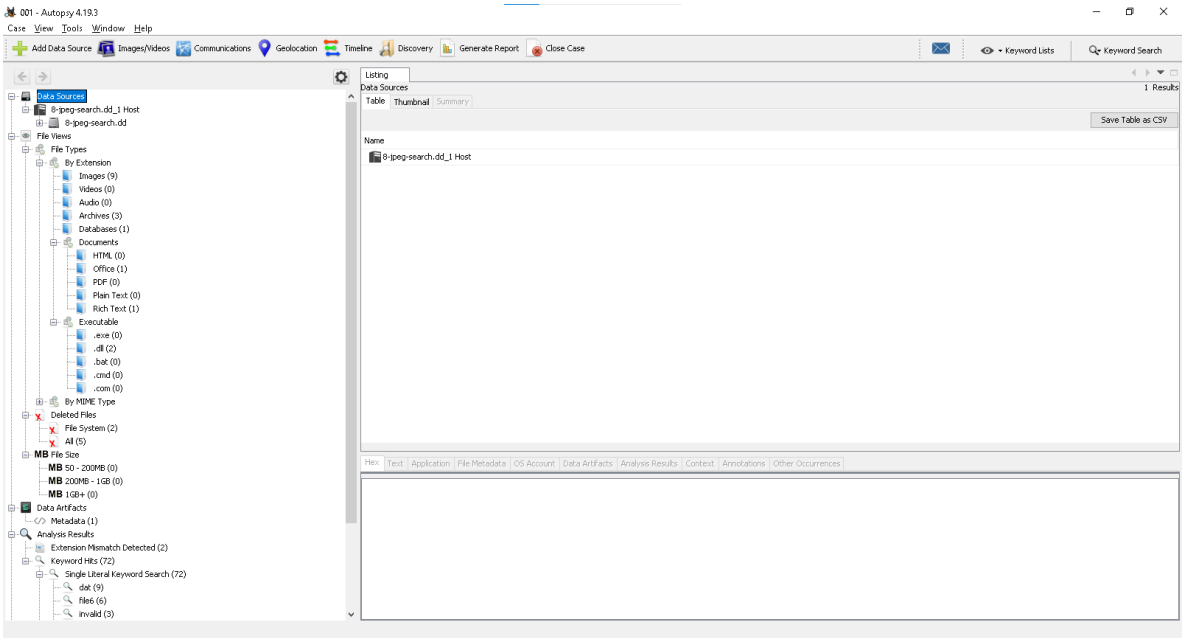
Nota: esta ilustración hace referencia la herramienta FTK Imager, fuente autoridad propia

6.4 Autopsy

Aplicación que recopila múltiples herramientas de análisis forense para el estudio de archivos, imágenes y discos duros la cual provee opciones sobre información de estructura previa de los archivos y datos eliminados.

Gracias a (Leandro, 2020) Autopsy es una plataforma digital forense de código abierto. Analiza discos rígidos, tarjetas de memoria, celulares y otros dispositivos de almacenamiento de datos, se destaca por su facilidad de uso, rapidez de resolución y plugins para realizar numerosas tareas específicas.

Ilustración 2 Interfaz de Autopsy



Nota: esta ilustración hace referencia la herramienta Autopsy, fuente autoridad propia

6.5 Volcado de Memoria

Es una captura tomada de la información que estaba procesando la memoria ya sea de un programa o archivo en específico o todo el sistema.

Según (Astrologypage, 2022) volcado de memoria es un proceso en el que los contenidos de la memoria se muestran y almacenan en caso de una falla de la aplicación o del sistema.

Memory dump ayuda a los desarrolladores de software y administradores de sistemas a diagnosticar, identificar y resolver el problema que provocó la falla de la aplicación o del sistema.

6.6 MAGNET RAM Capture

Aplicación que permite tomar una captura de la información que estaba siendo utilizada por la memoria RAM.

(Ram, 2018) Es una herramienta gratuita de la empresa Magnet Forensics que no requiere instalación, muy liviana (286 KB) y fácil de usar. Permite capturar la memoria RAM de sistemas Windows antiguos y modernos, ya sea de 32 bit que de 64 bit.

6.7 MAGNET Web Page Saver

Es una aplicación que permite tomar una captura de la información de una página web en el momento que se desee la captura de la información ofrece información como el enlace y la información imbuida en las imágenes y videos guardados de la página web.

MAGNET Web Page Saver (v3.3 lanzado el 17 de septiembre de 2020) es una herramienta perfecta para capturar cómo se ven las páginas web en un momento específico. Esto es especialmente útil en situaciones en las que las páginas web deben mostrarse en un entorno donde el acceso a Internet no está disponible (como la sala de un tribunal). (Forensics, 2020).

6.8 Antecedentes Científicos

La informática forense recolecta y utiliza evidencia digital para casos de delitos informáticos y para otro tipo de crímenes usando técnicas tecnológicas avanzadas. Un experto en informática forense utiliza estas técnicas para descubrir evidencia de un dispositivo de almacenamiento electrónico. Los datos pueden ser de cualquier clase de dispositivo electrónico como discos duros, discos compactos, discos flexibles, cintas de respaldo, computadoras portátiles, memorias extraíbles, archivos y correos electrónicos. (Bastillos, 2009).

6.9 Firma Digital

Herramienta de encriptado de información para la validación de seguridad entre archivos y programas.

Una firma digital es un dato en formato electrónico que sirve como mecanismo para verificar la autenticidad e integridad de otro dato también en formato electrónico (a este último, nos referiremos como dato firmado). Una firma digital es un tipo de firma electrónica generada por un procedimiento criptográfico que establece una relación única y exclusiva entre el dato firmado y el firmante. De forma simplificada, podemos describir este procedimiento como una caja negra que requiere como entradas un dispositivo seguro y el dato a ser firmado, generando como salida una firma digital (Cuno, 2015).

6.10 MD5

Opción de encriptación que utiliza hash de 128 bits que permite asegurar la valides de un archivo o si ha sufrido cambios.

MD5 (Message-Digest Algorithm 5 o Algoritmo de Firma de Mensajes 5): Desarrollado por Ron Rivest, y ha sido hasta los últimos años el algoritmo hash más usado. Procesa mensajes de una longitud arbitraria en bloques de 512 bits generando un compendio de128 bits. Debido a la capacidad de procesamiento actual esos 128 bits son insuficientes, además de que una serie de ataques criptoanalíticos han puesto de manifiesto algunas vulnerabilidades del algoritmo. Puede ser útil para comprobar la integridad de un fichero tras una descarga, por ejemplo, pero ya no es aceptable desde el punto de vista criptoanalítico. (Torres, 2011).

6.11 Filtrado de Información Informática

Es un acto en donde datos o información sensible ha sido adquirida por personas externas o sin ninguna relación a estos.

El término filtrado de información es usado frecuentemente para describir procesos que involucran la entrega de información a las personas que la necesitan, en aplicaciones como el correo electrónico o sistemas de distribución de multimedia, entre otros, pero no existe una clara diferenciación con otros procesos relacionados como recuperación, direccionamiento, categorización y extracción. (Monroy, 2003).

6.12 Revelación de Secretos Informáticos sin Autorización

Delito de revelación de secretos informáticos, es el más preocupante en virtud de que se trata del acceso no autorizado y de manera ilegal a un dispositivo computacional utilizando diversas estrategias y métodos que los delincuentes informáticos perfeccionan haciendo uso del avance tecnológico y sus conocimientos técnicos en el área de la informática con el fin de obtener secretos que afecta de gran manera a la víctima. (Ordoñez Mariscal, 2020).

6.13 Abuso de Confianza Informáticos sin Autorización

El articulo Penal 269C describe que todo acto realizado con el fin de interceptar datos será tomado como un ataque a la violación de los derechos y deberá ser retenido.

6.14 Manager Departamento Tecnológico

Un mánager TI es la persona encargada de que la comunicación entre los diferentes departamentos de trabajo funcione sin contratiempos y de manera eficaz.

6.15 Espionaje Informático

Este delito contra la seguridad del Estado se encuentra tipificado en el artículo 463 así: El que indebidamente obtenga, emplee o revele secreto político, económico o militar relacionado con la seguridad del Estado, incurrirá en prisión de cuatro (4) a doce (12) años. (Los delitos informáticos y su aplicación en la legislación colombiana, 2010).

6.16 Herramientas anti forenses

Las herramientas o técnicas anti forenses se definen según (Harris, 2006) como "cualquier intento de comprometer la disponibilidad de la evidencia para un proceso forense." Del mismo modo si se profundiza un poco más en este concepto y se desarrolla en términos más técnicos se genera la siguiente definición: "Cualquier intento exitoso efectuado por un individuo o proceso que impacte de manera negativa la identificación, la disponibilidad, la confiabilidad y la relevancia de la evidencia digital en un proceso forense". (Botero, 2009).

6.17 Windows Artifacts

Cuando un dispositivo de almacenamiento USB, como una memoria USB, se conecta a un sistema Windows, se crean varios identificadores en el sistema. Estos identificadores, o artefactos, persisten incluso después de que se haya cerrado el sistema. En muchos casos, estos artefactos pueden usarse con fines forenses para identificar dispositivos específicos que se han conectado a los sistemas Windows en cuestión. (Carvey, 2005).

6.18 Windows Event Logs

Artefactos que contienen marcas de tiempo al tallar datos en porciones no asignadas del sistema de archivos y posiblemente archivos de intercambio o hibernación. La elección de recuperar una cantidad significativa de artefactos con marca de tiempo y registros de eventos de interés en un compromiso forense comercial puede depender en gran medida de la viabilidad de los métodos de recuperación. (Murphey, 2007).

6.19 Content Disarm and Reconstruction

Desarmado y reconstrucción de contenido (CDR), también conocido como Extracción de amenazas, protege de manera proactiva contra amenazas conocidas y desconocidas contenidas en documentos mediante la eliminación de contenido ejecutable. La solución es única porque no

depende de la detección como la mayoría de las soluciones de seguridad. Cualquier contenido ejecutable dentro de un documento se elimina, ya sea que se detecte o no como una amenaza potencial para el usuario. Esto permite que CDR ofrezca una verdadera prevención de día cero, mientras entrega archivos a los usuarios rápidamente. (CheckPoint, 2020).

6.20 Apple Icloud

ICloud.com ofrece acceso en línea y control sobre las administraciones de Icloud. Apple expresa que 5GB es el almacenamiento más extremo disponible para cada cliente de Icloud. Incorpora información del correo, archivos también fotografías y grabaciones en la biblioteca de Fotos. (Icloud realiza un seguimiento de sus compras en la tienda de iTunes, por lo que otros dispositivos tienen la sustancia. Sea como fuere, la música, las aplicaciones y las películas de iTunes, al igual que los libros, no representan una marca en la web accesible. -capacidad basada. (Mobile, 2021).

6.21 Google Drive

Un servicio para, por un lado, almacenar de manera gratuita archivos en línea de hasta cinco gigabytes y, por otro, crear documentos de ofimática en línea, con la posibilidad de trabajar de manera colaborativa, sincrónica o asincrónica. En el listado de las 100 mejores herramientas para el aprendizaje -Top 100 Tools for Learning- del Centre for Learning & Performance Technologies aparece, en tercera posición, solo superada por la herramienta para microblogging Twitter y el conocido YouTube. (Castellanos Sánchez, 2013).

7. Marco Metodológico

Tabla 1 Contenido de Imagen 'DD'

Computador Personal - Imagen ‘DD’	
Objeto	Información detallada
Nombre_del_ archivo	cfreds_2015_data_leakage_pc
MD5	A49D1254C873808C58E6F1BCD60B5BDE
SHA-1	AFE5C9AB487BD47A8A9856B1371C2384D44FD785
Editor de imágenes	FTK Imager 3.4.0.1
Formato de imagen	DD Convertido de VMDK (algunos sectores no se pudieron recuperar)
Compresión	La más compacta posible
Bytes por sector	512
Sectores totales	41,943,040
Espacio total	20.00 GB (21,474,836,480 bytes)
Espacio Comprimido	5.05 GB (5,427,795,228 bytes) Comprimido usando 7zip

Nota: esta tabla hace referencia a información relevante acerca de la imagen del computador personal usado por el sujeto Iaman Informant como tamaño de la imagen MD5, SHA-1 y sectores totales

Tabla 2 Contenido de Imagen 'EnCase'

Computador Personal - Imagen ‘EnCase’	
Objeto	Información detallada
Nombre_del_ archivo	cfreds_2015_data_leakage_pc
MD5	A49D1254C873808C58E6F1BCD60B5BDE
SHA-1	AFE5C9AB487BD47A8A9856B1371C2384D44FD785
Editor de imágenes	EnCase Imager 7.10.00.103
Formato de imagen	E01(Experto es testigo del formato de compresión) convertida del archivo anterior a Imagen ‘DD’
Compresión	La más compacta posible
Bytes por sector	512
Sectores totales	41,943,040
Espacio total	20.00 GB (21,474,836,480 bytes)
Espacio Comprimido	7.28 GB (7,825,209,454 bytes) Comprimido usando 7zip

Nota: esta información hace referencia los datos relevantes de la imagen ‘EnCase’ contenido nombre del archivo, MD5, SHA-1, Formato de imagen, Compresión y espacio total

Tabla 3 Contenido de Imagen 'EnCase' RM#1

Medio Removible #1(RM#1) - Imagen ‘EnCase’	
Objeto	Información detallada
Nombre_del_ archivo	cfreds_2015_data_leakage_rm#1
MD5	8BFA4230BF4E35DB966B8C1A9321A0B1
SHA-1	F6BB840E98DD7C325AF45539313FC3978FFF812C
Editor de imágenes	FTK Imager 3.3.0.5 (Escritura bloqueada por Tableau USB Puente T8-R2)
Formato de imagen	E01 (Experto es testigo del formato de compresión)
Compresión	La más compacta posible
Bytes por sector	512
Sectores totales	7,821,312
Espacio total	3.7 GB (4,004,511,744 bytes)
Espacio Comprimido	74.5 MB (78,186,742 bytes)

Nota: Esta información hace referencia a la imagen ‘EnCase’ RM#1 Contenido nombre del archivo, MD5, SHA-1, Formato de imagen, Compresión y espacio total

Tabla 4 Contenido de Imagen 'DD' RM#2

Medio Removible #2(RM#2) - Imagen ‘DD’	
Objeto	Información detallada
Nombre_del_ archivo	cfreds_2015_data_leakage_rm#2
MD5	B4644902ACAB4583A1D0F9F1A08FAA77
SHA-1	048961A85CA3ECED8CC73F1517442D31D4DCA0A3
Editor de imágenes	FTK Imager 3.3.0.5 (Escritura bloqueada por Tableau USB Puente T8-R2)
Formato de imagen	E01 (Experto es testigo del formato de compresion)
Compresión	La más compacta posible
Bytes por sector	512
Sectores totales	7,821,312
Espacio total	3.7 GB (4,004,511,744 bytes)
Espacio Comprimido	219 MB (229,899,285 bytes) Comprimido usando 7zip

Nota: Esta información hace referencia a la imagen ‘DD’ RM#2 Contenido nombre del archivo, MD5, SHA-1, Formato de imagen y espacio total

Tabla 5 Contenido de Imagen 'RAW / CUE' RM#2

Medio Removible #2(RM#2) - Imagen ‘EnCase’	
Objeto	Información detallada
Nombre_del_ archivo	cfreds_2015_data_leakage_rm#2
MD5	B4644902ACAB4583A1D0F9F1A08FAA77
SHA-1	048961A85CA3ECED8CC73F1517442D31D4DCA0A3
Editor de imágenes	EnCase Imager 7.09.00.111 (Escritura bloqueada por Tableau USB Puente T8-R2)
Formato de imagen	E01 (Experto es testigo del formato de compresion)
Compresión	La más compacta posible
Bytes por sector	512
Sectores totales	7,821,312
Espacio total	3.7 GB (4,004,511,744 bytes)
Espacio Comprimido	243 MB (255,051,328 bytes)

Nota: esta información hace referencia a la Imagen ‘EnCase’ RM#2 Contenido nombre del archivo, MD5, SHA-1, formato de Imagen y espacio total

Tabla 6 Contenido de Imagen 'RAW / CUE' RM#3

Medio Removible #3(RM#3) - Imagen ‘RAW / CUE’	
Objeto	Información detallada
Nombre_del_ archivo	cfreds_2015_data_leakage_rm#three_type1
MD5	858C7250183A44DD83EB706F3F178990
SHA-1	471D3EEDCA9ADD872FC0708297284E1960FF44F8
Editor de imágenes	FTK Imager 3.3.0.5
Formato de imagen	RAW ISO / CUE (algunas veces BIN / CUE)
Bytes por sector	2,048
Sectores totales	52,514
Espacio total	102.57 MB (107,548,672 bytes)
Espacio Comprimido	92.8 MB (97,311,442 bytes) Comprimido Usando 7zip

Nota: esta información hace referencia a la imagen ‘RAW / CUE’ Contenido: nombre del archivo, MD5, SHA-1, Formato de Imagen y Espacio total.

Tabla 7 Contenido de Imagen 'DD'RM#3

Medio Removible #3(RM#3) - Imagen ‘DD’	
Objeto	Información detallada
Nombre_del_ archivo	cfreds_2015_data_leakage_rm#3_type2
MD5	858C7250183A44DD83EB706F3F178990

SHA-1	471D3EEDCA9ADD872FC0708297284E1960FF44F8
Editor de imágenes	FTK Imager 3.3.0.5 + bchunk
Formato de imagen	DD Convertida de 'RAW / CUE' usando bchunk
Bytes por sector	2,048
Sectores totales	52,514
Espacio total	102.57 MB (107,548,672 bytes)
Espacio Comprimido	78.6 MB (97,311,442 bytes) Comprimido Usando 7zip

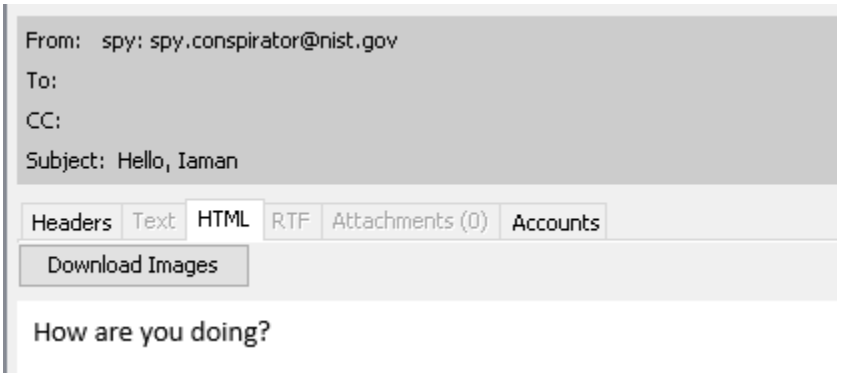
Nota: esta información hace referencia a la imagen 'DD' Contenido: nombre del archivo, MD5, SHA-1, Formato de Imagen y Espacio total.

Tabla 8 Contenido de Imagen 'EnCase' RM#3

Medio Removible #3(RM#3) - Imagen 'EnCase'	
Objeto	Información detallada
Nombre_del_ archivo	cfreds_2015_data_leakage_rm#3_type3
MD5	DF914108FB3D86744EB688EBA482FBDF
SHA-1	7F3C2EB1F1E2DB97BE6E963625402A0E362A532C
Editor de imágenes	EnCase Imager 7.09.00.111
Formato de imagen	E01 (Experto es testigo del formato de compresion)
Compresión	La más compacta posible
Bytes por sector	2,048
Sectores totales	52,513
Espacio total	102.56 MB (107,546,624 bytes)
Espacio Comprimido	90.21 MB (94,594,894 bytes)
Errores de lectura (Sector No.)	(321), (51,213), (51,233), (51,244), (51,265), (51,276), (51,297), (51,308), (51,329), (51,340), (51,361), (51,372), (51,393), (52,472), (52,481), (52,500)

Nota: esta información hace referencia a la imagen 'EnCase' Contenido: nombre del archivo, MD5, SHA-1, Formato de Imagen y espacio total

Ilustración 3 Primera Captura de pantalla del primer correo



Nota: esta imagen hace referencia a una Captura de pantalla del Primer correo con el agente externo, fuente autoridad propia.

Computador de escritorio pc (Dispositivo Principal utilizado para realizar el crimen)

Correos del sospechoso Iaman Informant Iaman.informant@nist.gov.ost

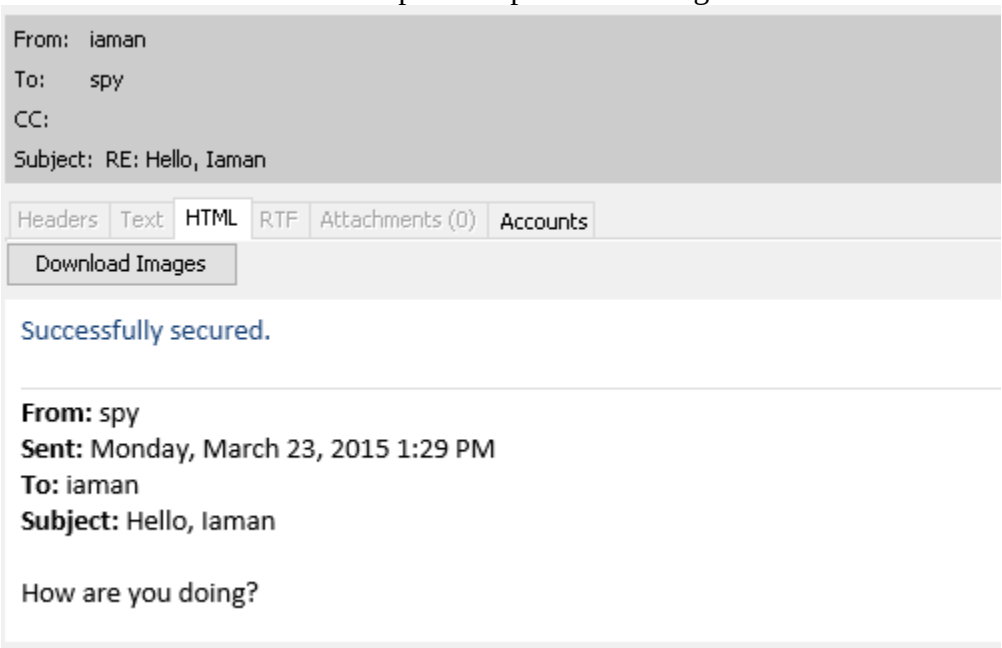
Correo del agente externo espía conspirador spy.conspirator@nist.gov.ost

Fecha 3/23/2015 Hora 13:44:00 COT

Iaman Informant responde el correo se puede confirmar que no es la primera vez que los dos sospechosos se conocen.

Iaman Informant responde al correo afirmando que tiene asegurado algo, pero no confirma que es.

Ilustración 4 Captura de pantalla del segundo correo

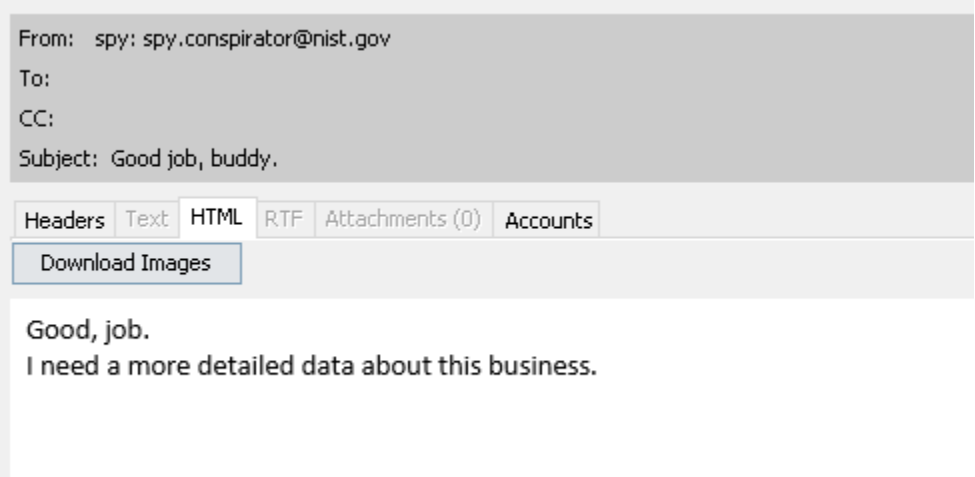


Nota: esta imagen hace referencia a la Respuesta al correo del espía conspirador, fuente autoridad propia.

Fecha 3/23/2015 Hora 14:15:00 COT

El agente externo espía conspirador responde al correo de Iaman Informant, felicitándolo por conseguir algo para a continuación decirle que necesita más datos detallados sobre el "negocio"

Ilustración 5 Captura de pantalla al tercer correo

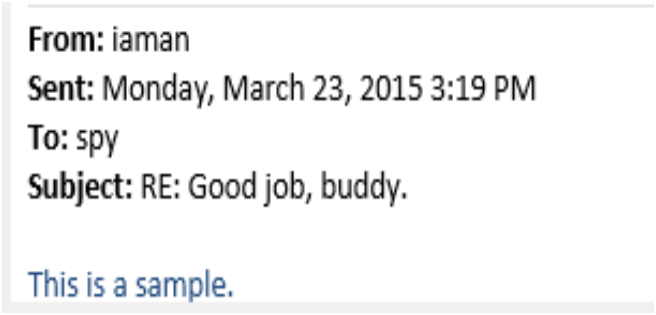


Nota: esta imagen hace referencia a la respuesta por correo del espía conspirador, fuente autoridad propia

Fecha 3/23/2015 Hora 14:19:00 COT

El sujeto Iaman Informant responde al correo de espía conspirador explicándole que la información enviada es solamente una muestra.

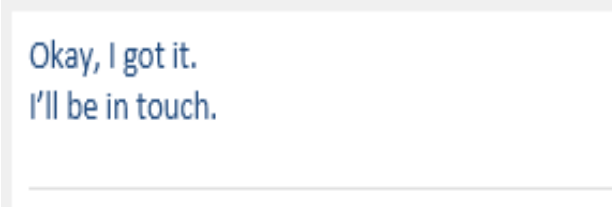
Ilustración 6 Captura de pantalla al cuarto correo



Nota: esta imagen hace referencia a la Respuesta al correo del espía conspirador, fuente autoridad propia.

El agente externo responde al correo explicando que entiende que la información que él recibió es solamente una muestra y afirma que estará en contacto con Iaman Informant.

Ilustración 7 Captura de pantalla al quinto correo

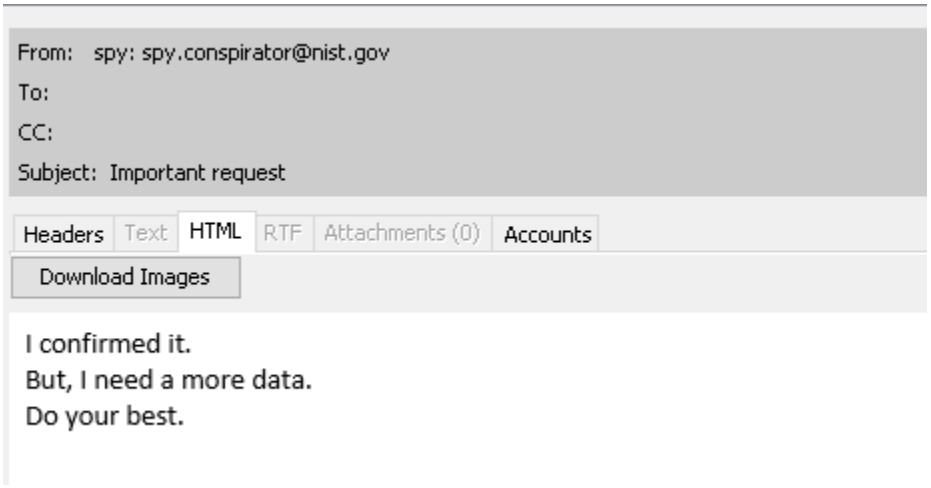


Nota: esta imagen hace referencia a la respuesta del espía conspirador al correo de Iaman Informant, fuente autoridad propia.

Fecha 3/23/2015 Hora 14:26:23 COT

El agente externo espía conspirador afirma que ha confirmado el valor de la información recibida por Iaman Informant, pero le explica que necesita más información y apoya Iaman Informant para que realice el trabajo de la mejor manera posible.

Ilustración 8 Captura de pantalla del sexto correo

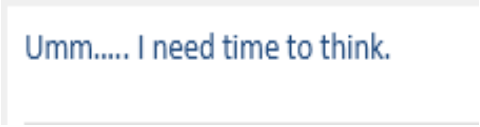


Nota: esta imagen hace referencia a la confirmación del valor de la información enviada por Iaman Informant, fuente autoridad propia

Fecha 3/23/2015 Hora 14:27:00 COT

El sujeto Iaman Informant responde al correo de Spy explicando que necesita más tiempo para pensarlo.

Ilustración 9 Captura de pantalla al séptimo correo



Nota: esta imagen hace referencia a la respuesta de Iaman Informant explica la situación al espía conspirador, fuente autoridad propia.

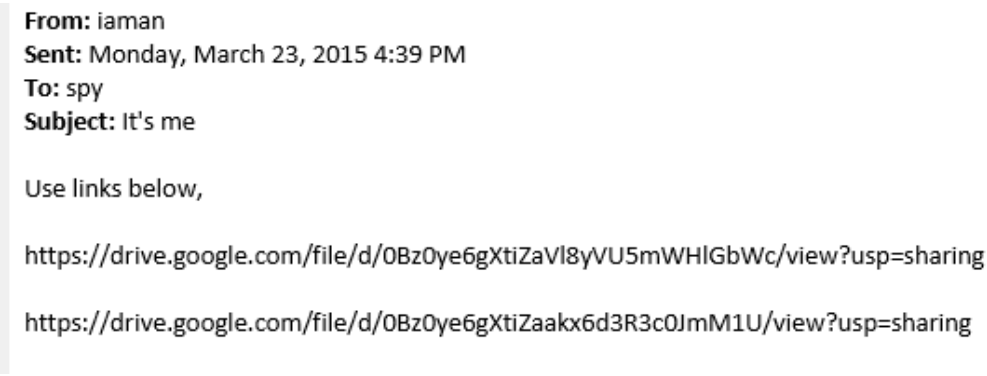
Fecha 3/23/2015 Hora 14:41:22 COT

Iaman Informant envía un correo a spy el cual tiene enlaces a archivos almacenados en la nube utilizando la herramienta Google Drive

Según Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMATICOS y el Artículo 269J. TRANSFERENCIA NO CONSENTIDA DE ARCHIVOS. aquí se puede evidencia que se

cometió el delito, por la persona Iaman Informant al transmitir información clasificada sobre proyectos de la empresa en la que trabaja a otro agente no involucrado o sin autorización de recibir dicha información.

Ilustración 10 Captura de pantalla al octavo correo


From: iaman
Sent: Monday, March 23, 2015 4:39 PM
To: spy
Subject: It's me

Use links below,

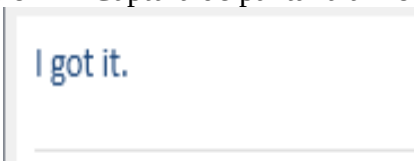
https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing

https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0JmM1U/view?usp=sharing

Nota: esta imagen hace referencia a los enlaces de archivos almacenados en Google Drive enviados por Iaman Informant, fuente autoridad propia.

Spy confirma que ha recibido la información

Ilustración 11 Captura de pantalla al noveno correo

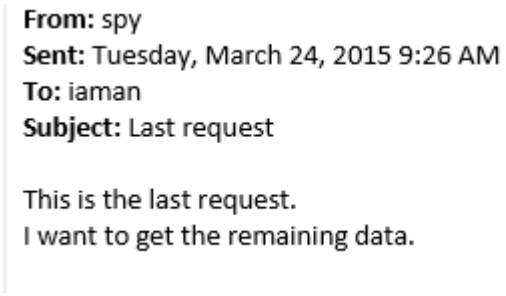

I got it.

Nota: esta imagen hace referencia a la confirmación sobre la información enviada por Iaman Informant, fuente autoridad propia.

Fecha 3/24/2015 Hora 08:25:59 COT

Iaman Informant recibe un correo de Spy en donde le afirma que es la última petición y que se le sea enviado los datos restantes.

Ilustración 12 Captura de pantalla décimo correo


From: spy
Sent: Tuesday, March 24, 2015 9:26 AM
To: iaman
Subject: Last request

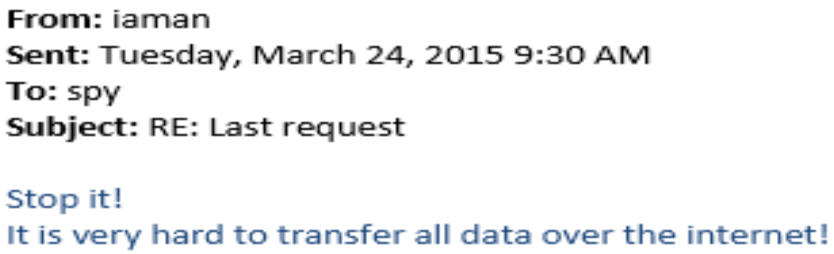
This is the last request.
I want to get the remaining data.

Nota: esta imagen hace referencia a la petición del espía conspirador para que se le sea enviado la información restante, fuente autoridad propia.

Fecha 3/24/2015 Hora 08:30:00 COT

Iaman Informant responde al correo de Spy afirmándole que se dé tenga que debido a que según el enviar toda la información por internet es muy difícil.

Ilustración 13 Captura de pantalla al onceavo correo


From: iaman
Sent: Tuesday, March 24, 2015 9:30 AM
To: spy
Subject: RE: Last request

Stop it!
It is very hard to transfer all data over the internet!

Nota: esta imagen hace referencia a la petición de Iaman Informant para que el espía conspirador no exija más información, fuente autoridad propia.

Fecha 3/24/2015 Hora 08:34:00 COT

Spy responde a Iaman Informant que no hay ningún problema y que la información puede ser enviada a través de otros medios como dispositivos de almacenamiento externos.

Ilustración 14 Captura de pantalla al doceavo correo

From: spy
Sent: Tuesday, March 24, 2015 9:34 AM
To: iaman
Subject: RE: Last request

No problem.
U can directly deliver storage devices that stored it.

Nota: esta imagen hace referencia a la respuesta del espía conspirador sobre que existen otras maneras en las que se puede entregar, autor elaboración propia.

Fecha 3/24/2015 Hora 08:35:00 COT
Iaman Informant responde a Spy que esta es la última vez que se le será enviada información

Ilustración 15 Captura de pantalla al treceavo correo

This is the last time..

Nota: esta imagen hace referencia a la respuesta de Iaman Informant en donde afirma que será la última vez que enviará información, fuente autoridad propia.

Fecha 3/24/2015 Hora 14:33:00 COT
Recibe otro correo de Spy en donde le explica que usar dispositivos USB suele ser fácil de detectar y que intente otro método.

Ilustración 16 Captura de pantalla al catorceavo correo

-----Original Message-----
From: spy
Sent: Tuesday, March 24, 2015 3:33 PM
To: iaman
Subject: Watch out!

USB device may be easily detected.

So, try another method.

Nota: esta imagen hace referencia al correo en donde espía conspirador le explica a Iaman Informant que los USB son fáciles de detectar, fuente autoridad propia.

Fecha 3/24/2015 Hora 14:34:00 COT

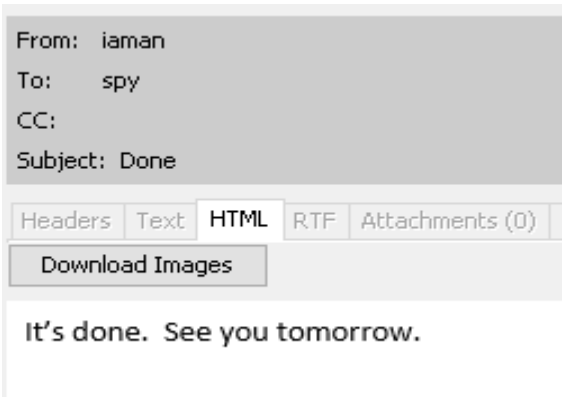
Iaman Informant responde al correo de Spy que lo está intentándolo

Ilustración 17 Captura de pantalla al quinceavo correo

Nota: esta imagen hace referencia a la respuesta de Iaman Informant de espía conspirador sobre intentar otro método, fuente autoridad propia.

Fecha 3/24/2015 Hora 16:05:00 COT
Iaman Informant envía un último correo a Spy para afirmar que la transferencia de los datos a otros dispositivos externos ya se ha terminado y que se encontrarán mañana
Según el Artículo 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES y el Artículo 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. La persona Iaman Informant, valiéndose de medios de almacenamiento externos transfirió información de secretos corporativos violando las conductas de los códigos penales de transferencia no autorizada de activos y evasión de medios de seguridad para entregárselas a otro agente conocido como espía conspirador.

Ilustración 18 Captura de pantalla al decimosexto correo

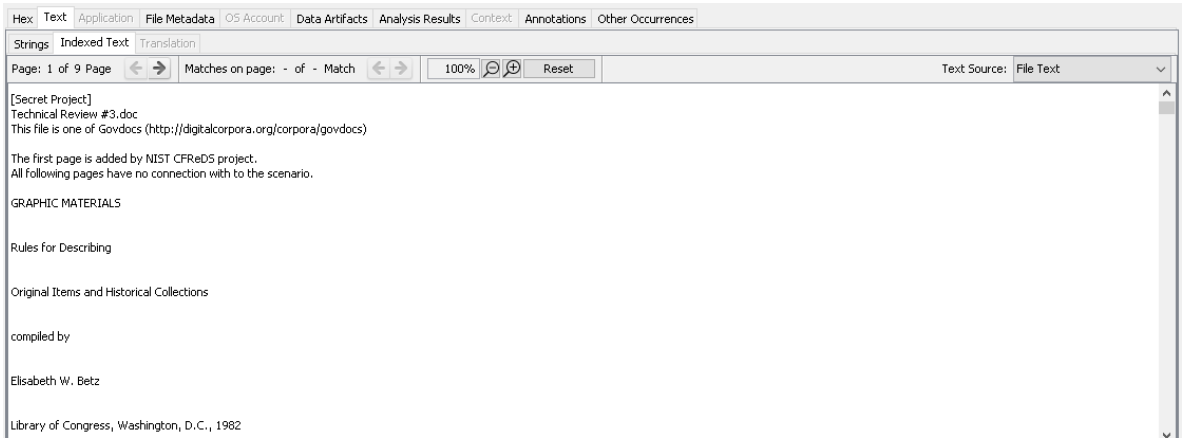


Nota: esta imagen hace referencia al correo de Iaman Informant en donde afirma que la información ya se ha terminado de transferir, fuente autoridad propia.

Fecha 3/25/2015 Hora 09:57:31 COT

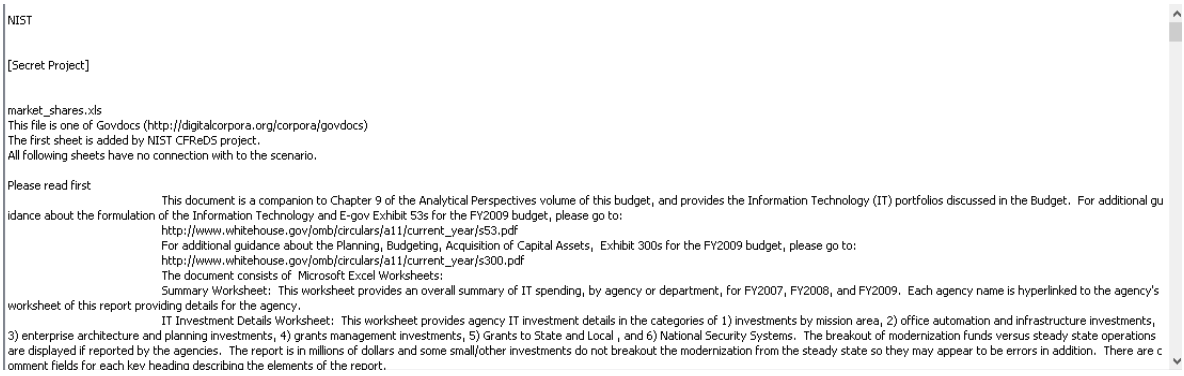
Iaman Informant descarga un software en su estación de trabajo el cual es Eraser, es una herramienta utilizada para eliminar rastros de actividad informática en dispositivos según el Artículo 269D. DAÑO INFORMÁTICO y el Artículo 269E. USO DE SOFTWARE MALICIOSO. La persona con el fin de ocultar los actos de la transferencia de archivos de manera no consentida, alteró y modificó la información del equipo Informático con el fin de ocultar el acto realizado.

Ilustración 19 Archivo.doc borrado sobre un proyecto



Nota: esta imagen hace referencia a un archivo Word sobre un proyecto que se estaba trabajando de manera interna en la empresa, fuente autoridad propia

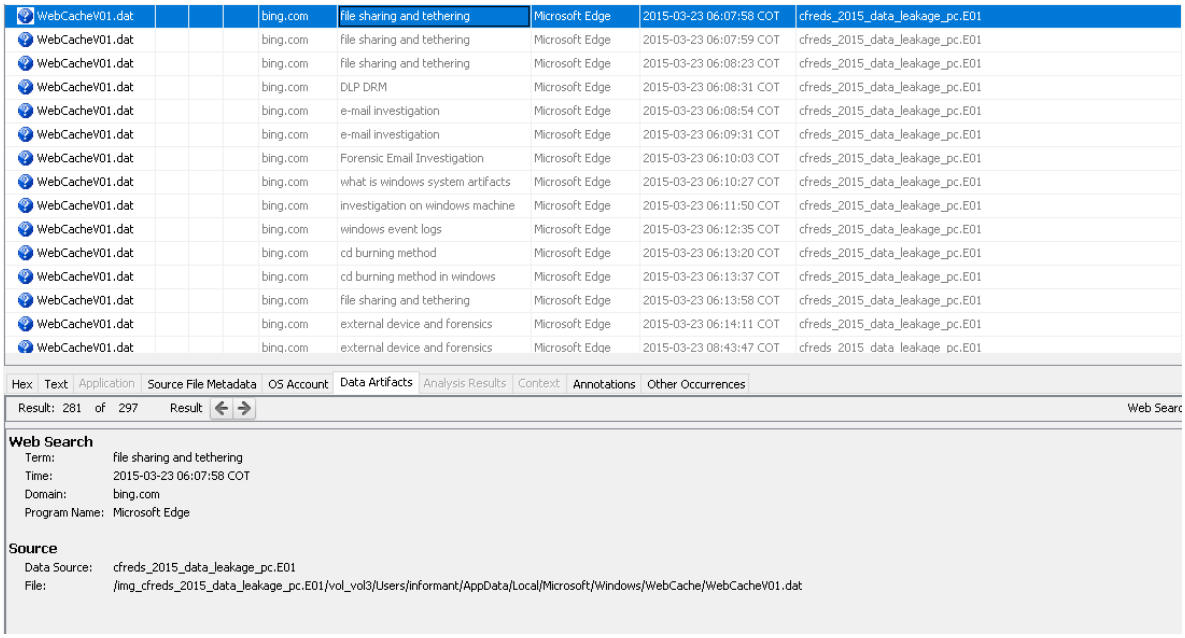
Ilustración 20 Archivo.xls sobre costos del proyecto



Nota: esta imagen hace referencia a un archivo Excel el cual contiene los costos de la creación del proyecto para la empresa, fuente autoridad propia

En base al artículo 269J. transferencia no consentida de activos y el artículo 269C, Interceptación de datos informáticos, la persona Iaman Informant sustrajo documentación relacionada sobre un proyecto que se estaba trabajando en secreto por la empresa, la documentación estaba conformada por archivos relacionados con la creación y el manejo de costos junto con información relacionada al proyecto que se estaba llevando a cabo, con esta información recolectada Iaman Informant transfirió copias de estos archivos a un dispositivo de almacenamiento externo conocido en el caso como RM#1 para luego borrar los archivos de su computador.

Ilustración 21 Búsquedas en la web sobre métodos para transferir información

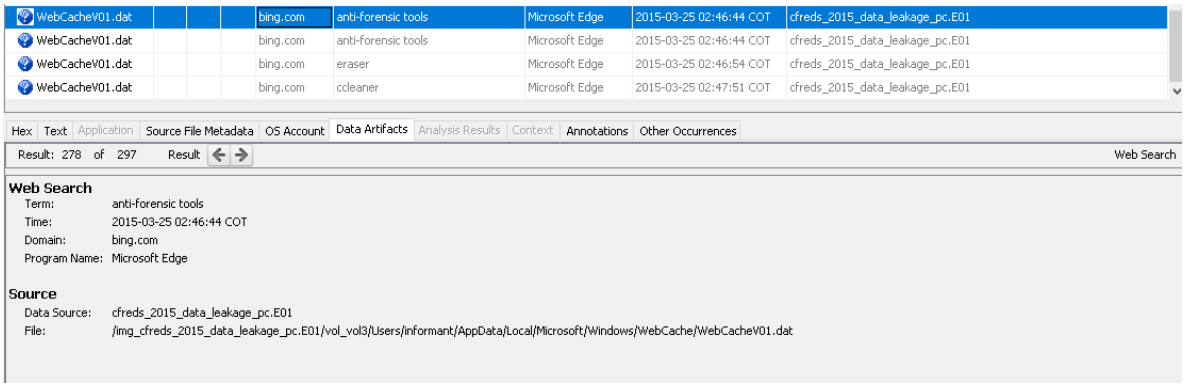


Nota: esta imagen hace referencia al historial web de Iaman Informant sobre transferencia de archivos, fuente autoridad propia.

Fecha 3/23/2015 Hora 06:07:58 COT

Durante una franja de tiempo de 8 horas aproximadamente se encontraron diferentes incidencias sobre búsquedas relacionadas con transferencia de información, métodos para fugar información, investigación forense enfocada en correos electrónicos, búsquedas sobre las herramientas que utiliza el sistema operativos Windows para catalogar las búsquedas hechas por un usuario, quemado de CD en Windows, fugar información, casos de fuga de información.

Ilustración 22 Búsquedas realizadas en la web de herramientas anti forense



Nota: esta imagen hace referencia a las búsquedas en la web sobre programas anti forense como se puede visualizar son Cleaner y Eraser, fuente autoridad propia

Fecha 3/25/2015 Hora 02:46:4 COT

Iaman Informant durante un corto periodo de tiempo de menos de 10 minutos realizó búsquedas en la web sobre programas antiforense, una vez terminadas estas búsquedas, decidió descargar dos programas con el objetivo de eliminar los rastros de su actividad en la computadora.

7.1 Línea de tiempo

Línea de tiempo del caso utilizando la herramienta https://www.visme.co
Fuente: Elaboración propia

Línea de tiempo del caso utilizando la herramienta https://www.visme.co
Fuente: Elaboración propia

Línea de tiempo del caso utilizando la herramienta https://www.visme.co
Fuente: Elaboración propia

Línea de tiempo del caso utilizando la herramienta https://www.visme.co
Fuente: Elaboración propia

su orientación específica a la investigación reconstructiva, de transgresiones que puedan o no de constituir ilícitos de diferente naturaleza penal (penal, civil, comercial, contractual, particular), involucra una enorme gama de autores y relaciones de todo tipo. Es inevitable el análisis metodológico ordenado y escrito de la legislación relacionada con esta en cada caso particular, no es posible describirlos a todo en una sola obra u definición, de ahí la necesidad del perito de acomodar su tarea a la jurisdicción y competencia a la cual debe actuar. (González, 2021)

El 2009 el código penal fue actualizado para cubrir ciertos aspectos de la nueva ola de ataques cibernéticos que no estaban siendo cubiertos por la versión anterior gracias a (oficial, 2009) por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

8.1 Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.(Ley N° 1273.Diario Oficial de la República de Colombia, 5 de enero 2009)

8.2 Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses. .(Ley N° 1273.Diario Oficial de la República de Colombia, 5 de enero 2009)

8.3 Artículo 269D. DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. (Ley N° 1273.Diario Oficial de la República de Colombia, 5 de enero 2009)

8.4 Artículo 269E. USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. (Ley N° 1273.Diario Oficial de la República de Colombia, 5 de enero 2009)

8.5 Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. .(Ley N° 1273.Diario Oficial de la República de Colombia, 5 de enero 2009)

8.6 Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere: 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. 2. Por servidor público en ejercicio de sus funciones 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este. 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro. 5. Obteniendo provecho para sí o para un tercero. 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional. 7. Utilizando como instrumento a un tercero de buena fe. 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales. .(Ley N° 1273.Diario Oficial de la República de Colombia, 5 de enero 2009)

8.7 Artículo 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio

semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código. (Ley N° 1273.Diario Oficial de la República de Colombia, 5 de enero 2009)

8.8 Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad. (Ley N° 1273.Diario Oficial de la República de Colombia, 5 de enero 2009)

9. Conclusiones

Se realizó este tipo de investigación donde se encontró al acusado culpable de varios tipos de delitos informáticos y violación con algunas políticas de la empresa donde presentaba sus labores. Teniendo en cuenta la metodología que se utilizó en las fases de Preservación de la evidencia, Análisis de la evidencia, Documentación y presentación de los resultados, para el análisis forense bajo una herramienta eficaz llamada Autopsy que permite ver archivos, imágenes, discos duros y toda la información eliminada en cierto tiempo. Para este paso se tuvo en cuenta lo que nos transmitió el taller de investigación digital forense, en donde se emplearon métodos científicos que fueron comprobables para preservar, recolectar, validar, identificar, analizar, interpretar, documentar y presentar evidencias digitales procedentes de fuentes digitales con el propósito de hacer posible la reconstrucción de hechos considerados delictivos, en donde se presentaron los siguientes hechos que se detallan a continuación:

Según el Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS y el Artículo 269J. TRANSFERENCIA NO CONSENTIDA DE ARCHIVOS. aquí se puede evidencia que se cometió el delito, por la persona Iaman Informant al transmitir información clasificada sobre proyectos de la empresa en la que trabaja a otro agente no involucrado o sin autorización de recibir dicha información.

Según el Artículo 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES y el Artículo 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. La persona Iaman Informant valiéndose de medios de almacenamiento externos transfirió información de secretos corporativos violando las conductas de los códigos penales de transferencia no autorizada de activos y evasión de medios de seguridad para entregárselas a otro agente conocido como espía conspirador.

Iaman Informant descarga un software en su estación de trabajo el cual es Eraser, es una herramienta utilizada para eliminar rastros de actividad informática en dispositivos según el Artículo 269D. DAÑO INFORMÁTICO y el Artículo 269E. USO DE SOFTWARE MALICIOSO. La persona con el fin de ocultar los actos de la transferencia de archivos de manera no consentida, alteró y modificó la información del equipo informático con el fin de ocultar el acto

realizado.

No obstante, el sujeto llamado Iaman Informant, el cual trabajaba como gerente de la división de una famosa empresa internacional, dedicada a desarrollar tecnologías y dispositivos de última generación violó estos y muchos más artículos referentes a la fuga de datos.

10. Recomendaciones

Utilizar almacenamiento en la nube Privada ya que se trata de una empresa, una forma de proteger toda la información privilegiada, transfiriéndose a través de internet u otra red, así los servidores remotos se ocupan del procesamiento y almacenamiento.

Implementación de una intranet en los diferentes departamentos que conforman las empresas, es una alternativa útil que se puede usar en empresas para compartir recursos de manera segura y privada.

Implementar sistemas de información de alta seguridad para aumentar la seguridad de la privacidad de los datos mediante el uso de criptografía permite cifrar, descifrar, privatizar toda la información y por otra parte está la estenografía, que utiliza comunicación encubierta para ocultar los mensajes de manera inteligente

Lista de Referencias

- Astrologypage, t. (2022). que es un volcado de memoria . Obtenido de https://es.theastrologypage.com/memory-dump

- Bastillos, X. E. (2009). MÉTODO INFORMÁTICO FORENSE PARA EL MANEJO ADECUADO DE LA EVIDENCIA DIGITAL Y SU ADMISIBILIDAD EN SITUACIONES JURÍDICAS EN BOLIVIA. Obtenido de https://repositorio.umsa.bo/bitstream/handle/123456789/1269/T-1739.pdf?sequence=1&isAllowed=y

- Botero, A. C. (2009). Técnicas Anti-Forense Em Informática: Ingeniería Reversa Aplicada a TimeStomp. Obtenido de Recuperado de: http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia3-Sesion6(3).pdf

- Carvey, H. &. (2005). Tracking USB storage: Analysis of windows artifacts generated by USB storage devices. Obtenido de Recuperado de: https://www.sciencedirect.com/science/article/abs/pii/S1742287605000320

- Castellanos Sánchez, A. &. (2013). Trabajo en equipo con Google Drive en la universidad online. Innovación educativa. Obtenido de Recuperado de: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-26732013000300006

- CheckPoint. (2020). What is Content Disarm and Reconstruction (CDR)? Obtenido de Recuperado de: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-content-disarm-and-reconstruction-cdr/

- CONFERENCE, D. F. (8 de agosto de 2001). dfrws. Obtenido de https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf

- Cuno, A. (2015). Conceptos de Firma Digital. IDENTIDAD DIGITAL. Obtenido de : https://www.researchgate.net/profile/Registro-De-Identificacion-Y-Estado-Civil/publication/351224030_Identidad_digital_La_identificacion_desde_los_registros_parroquiales_al_DNI_electronico/links/608b8c3d299bf1ad8d68fe35/Identidad-digital-La-identificacion
- Enrique, A. L. (1 de abril de 2012). La cadena de custodia informático-forense. Obtenido de https://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/45/42

- Forensics, M. (17 de septiembre de 2020). MAGNET Web Page Saver. Obtenido de https://www.magnetforensics.com/resources/web-page-saver/

- González, M. E. (2021). Manual de informatica Forense(Prueba indicaria informatico forense). Obtenido de https://books.google.es/books?hl=es&lr=&id=qIkxEAAAQBAJ&oi=fnd&pg=PT313&dq=antecedentes+cientificos+informatica+forense&ots=G0K3vnJO_L&sig=_ocZ0MBasVq

sUbE8MBTuLEfO5Po#v=onepage&q=antecedentes%20cientificos%20informatica%20forense&f=false

- Herrera, S. M. (2018). SABOTAJE INFORMÁTICO: ¿LA EXIGENCIA DE DAÑO GRAVE COMO ELEMENTO. Obtenido de https://www.researchgate.net/profile/Samuel-Herrera-3/publication/328642554_2018_SABOTAJE_INFORMATICO_LA_EXIGENCIA_DE_DANO_GRAVE_COMO_ELEMENTO_DEL_INJUSTO_En_Revista_Juridica_del_Ministerio_Publico_N_72_pp_143-171/links/5bd9f8fd4585150b2b945482/2018-SABOT

- Insectra. (2021). FTK Imager. Obtenido de https://www.insectraforensics.com/FTK-Imager

- Integral, G. a. (2019). Laboratorio de informatica forense. Obtenido de https://www.atlas.com.co/laboratorio-de-Informatica-forense

- Leandro. (2020). Tus Clases. Obtenido de autopsy una herramienta de analisis digital forense: https://www.tusclases.com.ar/blog/autopsy-herramienta-analisis-digital-forense

- Los delitos informáticos y su aplicación en la legislación colombiana. (2010). Recuperado de: https://hdl.handle.net/10901/6085.

- Mobile, M. C. (2021). Apple iCloud functions. Obtenido de Recuperado de: https://www.mycountrymobile.com/2021/10/15/apple-icloud-functions/

- Monroy, O. L. (2003). Análisis de la combinación de modelos de filtrado de información. Obtenido de Recuperado de: http://hdl.handle.net/20.500.12749/3331.

- Murphey, R. (2007). Automated Windows event log forensics. Obtenido de Recuperado de: https://www.sciencedirect.com/science/article/pii/S174228760700045X

- oficial, D. (2009). LEY 1273 DE 2009. Obtenido de Recuperado de: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

- Ordoñez Mariscal, L. H. (17 de Febrero de 2020). Obtenido de LA NECESIDAD JURÍDICA DE TIPIFICAR COMO DELITO LA REVELACIÓN DE SECRETOS INFORMÁTICOS: Recuperado de: http://hdl.handle.net/123456789/17876

- Ordoñez Mariscal, L. H. (s.f.). A NECESIDAD JURÍDICA DE TIPIFICAR COMO DELITO LA REVELACIÓN DE SECRETOS INFORMÁTICOS EN LA LEGISLACIÓN PENAL BOLIVIANA. Obtenido de Recuperado de http://hdl.handle.net/123456789/17876

- Ram, A. f. (octubre de 2018). Mendillo Vicenzo. Obtenido de http://mendillo.info/forensica/Análisis%20forense%20de%20la%20memoria%20RAM%20-%20V.%20Mendillo.pdf

- Torres, J. G. (Noviembre de 2011). ESTUDIO SOBRE LA IMPLEMENTACIÓN DE ENCRIPTACIÓN MD5 EN SITIOS WEB DURANTE EL FLUJO Y ALMACENAMIENTO DE CONTRASEÑAS. Obtenido de http://repositorio.uisrael.edu.ec/handle/47000/192

- Voutssas, M. (2010). Preservación documental digital y seguridad informática. Recuperado de:http://www.scielo.org.mx/pdf/ib/v24n50/v24n50a8.pdf

- Ambrustolo, M. (2020). Metodología de Implementación de un Sistema de Gestión de la Calidad en un Laboratorio Informático Forense.Grupo de Investigación y Extensión Mejora Continua, Calidad y Medio Ambiente, Facultad de Ingeniería. Universidad Nacional de Mar del Plata, Argentina,
Recuperado de: http://redi.ufasta.edu.ar:8082/jspui/handle/123456789/1744