UNIVERSIDAD AUTÓNOMA
"GABRIEL RENÉ MORENO"

FACULTAD DE CIENCIAS CONTABLES, AUDITORIA, SISTEMA DE CONTROL DE GESTION Y FINANZAS

INFORMATICA FORENSE

Universitario (a):

- Keyla Muriel Cruz Rueda 220018741
- Damaris Beltrán Choque 216100747
- Jhonny Fernández Cadena 218148089

Carrera: Contaduría Publica

Docente: Mario Gerardo Pinto Virhuez

Materia: Auditoría y Control de Sistema

Grupo: P

INDICE

I. OBJETIVOS DEL TRABAJO

- Aprobar la materia de auditoria control y sistemas
- Comprender todo el desarrollo del tema asignado por el docente
- Obtener mayor conocimiento del tema de informática forense investigado
- Explicar los fundamentos de la informática forense y su importancia en la investigación de delitos digitales.
- Describir las metodologías y herramientas utilizadas en el análisis forense digital.
- Identificar los principales retos y desafíos en la práctica de la informática forense.

II. INTRODUCCIÓN

Este trabajo de investigación es desarrollado por los estudiantes de la materia para mayor conocimiento del tema, de esta manera poder comprender todo lo relacionado a la informática forense. El cual nos indica que es de mucha importancia saber respecto a la informática forense ya que el mundo se conecta más de forma digital, para cometer delitos y estafar a las personas mediante redes.

De esta manera tanto la policía como los ministerios públicos tienen la necesidad de especializarse y capacitarse en esta nueva área que es la informática forense ya que es una ciencia que se ocupa de la utilización de los métodos científicos aplicables a la investigación de delitos, no solo informáticos y donde se utiliza el análisis forense de las evidencias digitales.

Esta disciplina se basa en el uso de técnicas y herramientas especializadas para la **recuperación de datos** de dispositivos como computadoras, teléfonos móviles, servidores y discos duros dañados o borrados, de manera que sea posible reconstruir eventos y situaciones relacionadas con un caso.

Uno de los principales retos de la informática forense es garantizar la **integridad de la evidencia digital**. Los expertos forenses deben seguir un proceso muy estricto para asegurar que los datos no se alteren, preservando así su validez en un contexto judicial. La cadena de custodia, que establece un registro detallado del manejo de la evidencia, es fundamental para lograr esto. Además, los analistas deben ser capaces de presentar sus hallazgos de manera clara y comprensible, incluso para aquellos que no tienen conocimientos técnicos.

El propósito de este trabajo es analizar la informática forense desde sus fundamentos hasta su aplicación en investigaciones, destacando su importancia legal y cómo las herramientas y técnicas modernas permiten una efectiva solución de delitos informáticos y otras infracciones relacionadas con el uso indebido de la tecnología.

III. JUSTIFICACION

La justificación de la informática forense reside en su capacidad para obtener y analizar evidencias digitales en investigaciones legales y de seguridad, así como para prevenir y responder a incidentes de ciberseguridad. Permite identificar, recopilar, preservar y analizar datos de forma que se preserve la integridad de la evidencia para su uso en procesos judiciales

La informática forense juega un papel fundamental en la investigación y persecución de los cibercriminales, pues su objetivo principal es la obtención de evidencias relativas a un crimen digital.

Es fundamental en la actualidad porque nos permite investigar y resolver delitos relacionados con la tecnología y la información digital. En un mundo donde la mayoría de las actividades, desde las financieras hasta las personales, dependen de dispositivos electrónicos, la capacidad de recopilar, analizar y preservar evidencia digital se vuelve esencial para garantizar la justicia y la seguridad.

Además, la informática forense ayuda a detectar fraudes, ciberataques, delitos cibernéticos y otros ilícitos, permitiendo a las autoridades actuar de manera efectiva y rápida. También contribuye a proteger a las empresas y a las personas, asegurando que los datos y la información confidencial estén seguros.

En Bolivia, como en muchos otros países, contar con profesionales y técnicas en informática forense fortalece el sistema judicial y la lucha contra el crimen digital, promoviendo un entorno más seguro y confiable en el uso de las tecnologías.

IV. OBJETIVOS DEL TEMA

OBJETIVO GENERAL

El objetivo principal de este tema es explicar qué es la informática forense, su proceso, las herramientas que se utilizan y cómo se lleva a cabo una investigación forense digital. Además, se discutirá la importancia de esta disciplina tanto en el ámbito judicial como en el corporativo, y cómo los avances tecnológicos han influido en su desarrollo

OBJETIVOS ESPECIFICOS

- Determinar si se ha cometido un delito informático.
- Adquirir la evidencia digital de manera forense y legalmente admisible.
- Examinar la evidencia digital para descubrir hechos relevantes para el caso.
- Asegurar que la evidencia no sea alterada durante el proceso.
- Atribuir las acciones a individuos o entidades específicas.
- Proporcionar pruebas sólidas y documentación para su uso en juicios, investigaciones internas o disputas legales.
- Utilizar la información obtenida para mejorar la seguridad y prevenir incidentes futuros.

V. DESARROLLO

LA INFORMATICA FORENCE

La informática forense, también conocida como ciencia forense digital, informática forense o ciberforense, combina la informática y la ciencia forense legal para recopilar pruebas digitales de una manera que sea admisible en un tribunal de justicia.

La informática forense está estrechamente relacionada con la ciberseguridad. Los hallazgos forenses informáticos pueden ayudar a los equipos de ciberseguridad a acelerar la detección y resolución de amenazas cibernéticas y a prevenir futuros ataques cibernéticos. Una disciplina de ciberseguridad emergente, análisis forense digital y respuesta ante incidentes (DFIR), integra análisis forense informático y actividades de respuesta ante incidentes para acelerar la corrección de las amenazas cibernéticas y, al mismo tiempo, garantizar que las pruebas digitales relacionadas no estén comprometidas.

PRINCIPIOS DE LA INFORMTICA FORENSE

Para el manejo y recolección de pruebas que se utilizan en el análisis forense digital de ciberataques o delitos informáticos, la Organización Internacional de Prueba Informática o *International Organization On Computer Evidence* (IOCE) establece los siguientes 5 principios:

1. Con respecto a la recolección de la evidencia computacional, las acciones tomadas no deben cambiar por ningún motivo esta evidencia.
2. Cuando es necesario que una persona tenga acceso a pruebas digitales originales, esa persona debe ser un profesional forense.
3. Toda la actividad referente a la recolección, acceso, almacenamiento o a la transferencia de la evidencia digital, debe ser documentada completamente en forma de un peritaje. Debe ser preservada y estar disponible para la revisión y el análisis forense informático.

4. Un individuo es responsable de todas las acciones tomadas con respecto a la evidencia digital, mientras que esta se encuentre bajo su posesión.
5. Cualquier agencia que sea responsable de recolectar, tener acceso, almacenar o transferir evidencia digital es responsable de cumplir con estos principios.

TIPOS DE INFORMÁTICA FORENSE

A pesar de que la informática forense es muy amplia, en la actualidad se puede clasificar de acuerdo al sitio en específico en el que se aplica. De esta forma encontramos los siguientes tipos de informática forense:

De sistemas operativos

En este caso, la informática forense se dedica a recuperar información, tales como archivos, contraseñas, información personal, desde el sistema operativo de un dispositivo, ya sea Windows, Mac iOS, Linux, entre otros.

Esta rama de la informática forense es de utilidad para encontrar una hoja de ruta directa hacia los datos almacenados en el disco duro, los cuales servirán como evidencia empírica del ciberatacante que ejecutó el robo de datos personales o información privada.

De redes

En la informática forense de redes, el analista o perito informático forense monitorea el tráfico de un activo de red y realiza un análisis de datos del mismo para así determinar el origen de los ataques cibernéticos, las vulnerabilidades del sitio y las medidas de seguridad necesarias para evitar que el ataque se repita en un futuro.

Este tipo de investigación forense suele ser utilizado por el departamento de tecnologías de la información (TI) para identificar tráfico sospechoso y, con ello, evitar que se lleven a cabo ataques informáticos.

De dispositivos móviles

En cuanto al análisis de dispositivos móviles, el objetivo es recuperar los datos que tengan el potencial de convertirse en evidencia digital que permita identificar al responsable del ataque dirigido a obtener información sensible del usuario final.

En estos casos se siguen protocolos en materia de ciberseguridad que permiten aislar los datos recuperados con gran precisión y efectividad.

En la nube

Esta es una de las ramas más novedosas en cuanto a los tipos de informática forense, ya que en los últimos años, se ha popularizado el uso de la nube para almacenar información.

En este caso, se combina el análisis forense digital y la computación en la nube para recuperar información sensible de servidores, aplicaciones, y cualquier tipo de recursos informáticos relacionados con la nube.

La informática forense abarca diversas áreas, desde la recopilación de datos en dispositivos electrónicos hasta el análisis detallado de sistemas y redes comprometidos. A continuación, se presentan los aspectos más relevantes:

1. Proceso de investigación forense digital
    - Identificación: Detección de fuentes de evidencia digital.
    - Preservación: Protección de la integridad de los datos recolectados.
    - Análisis: Evaluación de la información digital para determinar causas y responsabilidades.
    - Presentación: Elaboración de informes técnicos para su uso legal.
2. Herramientas utilizadas en informática forense
    - Software de análisis forense: FTK, EnCase, Autopsy.
    - Técnicas de extracción de datos: Análisis de discos duros, memoria RAM y dispositivos móviles.
    - Análisis de redes: Identificación de intrusiones y rastreo de actividades sospechosas.
3. Retos y desafíos en la informática forense

- Criptografía y ocultación de datos: Uso de cifrado para esconder información.
- Evolución tecnológica: Nuevas amenazas y sistemas complejos.
- Aspectos legales: Regulaciones y normativas para la obtención de evidencias digitales.

La informática forense es una disciplina en constante evolución que desempeña un papel fundamental en la seguridad informática y la lucha contra el cibercrimen. Su aplicación efectiva requiere conocimientos técnicos especializados y un marco legal adecuado para garantizar la validez de las evidencias recolectadas.

EL PROCESO FORENSE DIGITAL

El proceso de una investigación forense digital sigue una serie de pasos que aseguran que la evidencia obtenida sea válida y usable en el ámbito legal. Estos pasos incluyen:

1. **Identificación de la evidencia**: En esta fase, los investigadores determinan qué dispositivos y datos pueden contener evidencia relevante para el caso.
2. **Adquisición de los datos**: Se realiza una copia forense exacta de los datos de los dispositivos sin alterar la información original. Esta copia es una "imagen" bit a bit de los datos, que garantiza la exactitud de la evidencia.
3. **Preservación de la cadena de custodia**: La evidencia digital debe ser manejada cuidadosamente para mantener su integridad. Cada vez que la evidencia es transferida o manipulada, debe registrarse detalladamente para garantizar que no se haya alterado.
4. **Análisis de la evidencia**: Los analistas forenses examinan los datos obtenidos para identificar evidencia clave, como correos electrónicos, registros de navegación web, archivos eliminados o actividades sospechosas en los sistemas.
5. **Informe y presentación de resultados**: Finalmente, se redacta un informe detallado que explica los hallazgos, presentando la evidencia de manera

clara y comprensible para ser utilizada en procedimientos judiciales o decisiones corporativas.

POR QUÉ ES IMPORTANTE LA INFORMÁTICA FORENSE PARA EMPRESAS Y PARTICULARES

Prevención de incidentes y brechas de seguridad

Mediante un análisis forense informático, es posible identificar las vulnerabilidades de sistemas y redes domésticas y corporativas con fines preventivos. Y es que la denegación de servicio distribuido (DDoS), la inyección de SQL, los ataques de ransomware y otras clases de malwares pueden comprometer la información personal y de terceros.

Para las empresas y administraciones públicas, los expertos en informática forense desempeñan un rol clave en investigaciones de incidentes y brechas de seguridad, pues estas habilitan ‘fisuras’ en el sistema que permiten a los ciberdelincuentes acceder y sustraer información nuevamente.

Obtención de evidencias digitales

La escena del crimen digital es una realidad desconocida para la mayoría de los ciudadanos y organizaciones. La búsqueda de evidencias en dispositivos y unidades de almacenamiento —metadatos de imágenes, documentos, registros de chat, etcétera— forma parte del quehacer diario de los especialistas en informática forense, siendo un servicio al alza por el valor probatorio de dichas evidencias en procesos judiciales. Así, la importancia de la informática forense en el Derecho está fuera de duda.

Asesoría para víctimas de delitos telemáticos

Todas las predicciones y encuestas sobre ciberdelincuencia coinciden: las amenazas cibernéticas se acrecenterán en los próximos años, juntamente con los procesos judiciales que involucren ordenadores, móviles y dispositivos electrónicos. Además de poner en claro los ataques e infracciones relacionadas, el informático forense se implica en labores de asesoramiento jurídico.

En concreto, el perito informático estudia e informa de las consecuencias legales que una brecha de seguridad, ataque digital, etcétera, conlleva para la víctima. La cuestión es particularmente delicada para las empresas afectadas, pues en caso de sufrir una filtración de datos sensibles de su cartera de clientes o suscriptores, verbigracia, deben comunicarla a la Agencia Española de Protección de Datos (AEPD) en un plazo de 72 horas.

Así, y respondiendo al interrogante de cuál es la importancia de la informática forense en el mundo actual, la asesoría legal es otra razón de peso que justifican la demanda de esta disciplina en empresas y organismos públicos.

Salvaguarda de la reputación corporativa

La filtración de datos y otros ataques cibernéticos a empresas provocan una caída en el precio de sus acciones y una pérdida media de 257 millones de usuarios, según un estudio de Bitglass basado en datos de los incidentes de Marriott, Equifax y Yahoo entre 2016 y 2018. Para cualquier organización, tomar la precaución de realizar un análisis forense informático, y por tanto de blindar la seguridad de su negocio y de su cartera de clientes, permite salvaguardar su reputación frente a las amenazas digitales.

Geolocalización de dispositivos y accesos sospechosos

Los avances en informática forense permiten hoy la geolocalización y el seguimiento de cualquier actividad en entornos domésticos, empresariales e incluso militares. Con ello, se logra descubrir quién, cuándo y dónde se cometieron ilegalidades que involucraron a tabletas, móviles, ordenadores y otros dispositivos. Esta información, de ser verificada por peritos forenses, puede ser utilizada en procesos judiciales.

USOS DE LA INFORMÁTICA FORENSE

Debido a que la tecnología va creciendo con el pasar de los días, la informática forense ha cobrado más relevancia en cuanto a su utilidad. A continuación te hablaremos sobre los usos más comunes de la informática forense:

Prevenir ciberataques

Uno de los principales usos de la informática forense es realizar análisis exhaustivos de los sistemas informáticos para detectar vulnerabilidades que puedan convertirse en puertas de entrada para ciberatacantes. En este sentido, la informática forense es similar al hacking ético, y es considerada como una primera línea de defensa ante las amenazas cibernéticas.

En relación con lo anterior, Delta cuenta con un servicio llamado Apolo, que se encarga de automatizar y simplificar la ciberseguridad de tu empresa para evitar que sea susceptible a ciberataques que puedan poner en riesgo su funcionamiento.

Recolección de evidencias digitales

Por otro lado, es clave al momento de recuperar información importante de ordenadores, equipos o servidores que le sirven a las agencias de investigación para sustentar un caso y llevarlo a tribunales para hacer justicia.

De acuerdo a las evidencias recolectadas durante la investigación informática, es posible determinar el origen del ciberataque, los motivos del mismo y los ciberatacantes que llevaron a cabo el delito informático.

Detección de vulnerabilidades

La informática forense se encarga de realizar un análisis profundo de los sistemas para evaluar los puntos débiles que pueden servir como entrada de posibles ciberataques tales como ransomware, ataques de phishing, ataque DDoS, entre otros.

Este punto va más allá de simplemente instalar un software antivirus, ya que se emplean conocimientos técnicos avanzados para optimizar las defensas de los sistemas y disminuir las probabilidades de sufrir un ciberataque a corto y largo plazo.

Evaluar el desempeño laboral

En este caso, nos permite demostrar si un trabajador está cumpliendo correctamente con su labor dentro de la empresa. Se realiza un análisis exhaustivo del sistema de archivos de su ordenador para comprobar si está cumpliendo con los protocolos de la política de seguridad establecida.

Realizar investigaciones

Como se mencionó anteriormente, y de manera similar a lo que ocurre en otras ciencias forenses, las evidencias recolectadas por el perito informático forense son de utilidad para llevar a cabo investigaciones que revelen el origen del ciberataque que ha sufrido una empresa. Dicha información se emplea en investigaciones civiles que pueden tener como resultado una demanda.

HERRAMIENTAS BASICAS DE LA INFORMATICA FORENCE

Existen diversas herramientas forenses utilizadas para realizar cada una de las fases mencionadas. Algunas de las más comunes son:

- **Autopsy**: Herramienta gratuita que facilita el análisis de discos duros y otros medios de almacenamiento. Permite recuperar archivos eliminados y detectar actividad maliciosa.
- **FTK (Forensic Toolkit)**: Es una de las herramientas más completas, capaz de realizar un análisis exhaustivo de datos, incluyendo la recuperación de archivos y la identificación de rastros de actividad en el sistema.
- **EnCase**: Otra herramienta ampliamente utilizada en el ámbito forense, que permite realizar un análisis detallado de la evidencia digital y generar informes con fines legales.
- **Wireshark**: Utilizado para analizar el tráfico de red. Puede identificar patrones sospechosos, como intrusiones o transferencias no autorizadas de datos.

- **Volatility**: Específicamente diseñado para el análisis de la memoria RAM de un sistema, permitiendo identificar malware y rastros de actividad no detectados por otros métodos.

RELEVANCIA DE LA INFORMÁTICA FORENSE EN EL ÁMBITO LEGAL

La informática forense desempeña un papel crucial en la resolución de casos legales relacionados con delitos informáticos. Los tribunales y las autoridades judiciales deben confiar en que la evidencia digital presentada sea auténtica y no haya sido manipulada. Para ello, los expertos forenses deben seguir procedimientos estandarizados y presentar la evidencia de manera transparente.

Además de su uso en la resolución de delitos, la informática forense también juega un papel en las **auditorías corporativas**, donde se investiga el uso indebido de los sistemas informáticos dentro de una empresa o la filtración de datos sensibles.

Formación de informáticos forenses

Los criminales informáticos son una nueva generación de delincuentes, en este contexto, es necesario desarrollar un nuevo tipo de investigadores: los informáticos forenses. En este momento es un desafío encontrar personas que tengan este perfil, ya que no existen suficientes programas que realicen este tipo de formación. Adicionalmente, en este momento, la mayoría de las personas ignoran la importancia de los informáticos forenses porque no son conscientes de la dimensión del cibercrimen. Usualmente se cree que no es algo tan grave y se le da mayor importancia a otro tipo de crímenes.

Por lo tanto, se deben plantear programas e iniciativas para poder realizar esta formación. Según investigaciones e iniciativas ya realizadas, hay cuatro componentes principales que deben estar presentes en un programa de computación forense o forensia digital: contenido multidisciplinario, ejercicios prácticos, profesores de calidad y ejemplos del mundo real.

Contenido multidisciplinario: técnico en informática, conocimiento de criminalística, seguridad y delitos informáticos, entre otros.

Ejercicios prácticos en el laboratorio: con herramientas tecnológicas forenses, en diferentes niveles de dificultad y variedad de componentes a analizar.

Profesores calificados con alto conocimiento en el tema

Ejemplos del mundo real: con el fin de dar mayor profundidad al aprendizaje.

La informática forense es esencial para:

- Asegurar la integridad y disponibilidad de la infraestructura de red cuando sucede un incidente de ciberseguridad o ataque informático.
- Identificar y obtener evidencias de los cibercrímenes de manera apropiada.
- Asegurar la protección adecuada de los datos y el cumplimiento regulatorio.
- Proteger a las organizaciones para que no vuelvan a suceder en el futuro los incidentes ocurridos.
- Ayudar en la protección de crímenes online, como abusos, bullying…
- Minimizar las pérdidas tangibles o intangibles de las organizaciones o individuos relativas a incidentes de seguridad.
- Soportar el proceso judicial de enjuiciamiento de los criminales

Componentes clave de la informática forense

Recopilación de evidencias digitales

Recopilar la evidencia digital es uno de los pilares de la informática forense. Requiere un conocimiento amplio tanto de los sistemas informáticos, como de las técnicas de investigación forense.

Durante esta primera etapa, el perito informático identifica, preserva y recopila la evidencia digital. Para ello recurre a técnicas como la extracción de datos, análisis de registros, creación de imágenes forenses, entre otros. Estos procesos los debe hacer siguiendo protocolos estrictos para evitar que la evidencia se altere.

Análisis forense de dispositivos digitales

El informático forense toma los dispositivos involucrados en el caso y los analiza para encontrar evidencia relevante. Este proceso implica extraer los datos de los dispositivos, recuperar archivos, identificar los metadatos, detectar malware y tráfico sospechoso en las redes, etc.

Herramientas esenciales en informática forense

Con las herramientas adecuadas, los informáticos forenses pueden clonar discos duros, recuperar datos borrados, analizar archivos de imagen, descifrar contraseñas y examinar el tráfico de red. Estas herramientas permiten hacer un análisis meticuloso en cada dispositivo y evolucionan conforme lo hacen la tecnología y los crímenes cibernéticos.

Las etapas del análisis forense se dividen de la siguiente manera:

Preparación y evaluación de riesgos

En primer lugar, se determinan los sistemas que se van a investigar y se establecen los objetivos de la investigación. Para ello es necesario obtener información sobre el incidente, así como de los dispositivos que se han visto afectados o que pudieran estar involucrados.

Implica también la evaluación de riesgos, como la contaminación o pérdida de los datos. Asimismo, durante esta etapa se crea el plan que guiará la investigación. Es decir, el método que se seguirá, las herramientas a utilizar, quién se encargará del análisis.

Recogida y preservación de datos

Con el plan de investigación listo se procede a identificar los dispositivos que pueden tener alguna evidencia. Antes de continuar se deben aislar y protegerlos para evitar que se modifiquen o se eliminen datos.

Una vez que se protegen los dispositivos, se crean copias exactas de cada uno para analizarlos sin correr el riesgo de modificar la evidencia original. Durante todo este

proceso es imprescindible preservar la cadena de custodia para garantizar la integridad de la evidencia.

Análisis y extracción de datos

A continuación se analizan los datos forenses para identificar la evidencia digital relevante. Durante esta etapa se recuperan los archivos borrados, se identifica el tráfico y la presencia de malware, se evalúan los metadatos.

El informático forense analiza los datos extraídos para identificar las pistas que puedan conducir a la resolución del caso.

Documentación y presentación de hallazgos

Por último, se redacta el informe pericial. En este documento se detalla cómo se hizo el peritaje, los hallazgos que se encontraron y las conclusiones del perito.

Te puede interesar Qué hacer si has sido víctima de phishng los resultados se presentarán al cliente y, si es necesario, se presentará el testimonio del experto en audiencias judiciales.

CASOS INTERNACIONALES

1. Caso Enron (EE. UU., 2001)

Resumen: Enron manipuló sus balances contables para ocultar pérdidas.

Aplicación forense: Expertos recuperaron correos electrónicos y archivos eliminados que demostraban la manipulación de información financiera.

Resultado: Varios ejecutivos fueron condenados. Se impulsó el uso de la informática forense en auditorías corporativas.

2. Ataque a Sony Pictures (2014)

Resumen: Hackers robaron y filtraron películas, correos internos y datos personales.

Aplicación forense: Análisis de logs, malware y redes para rastrear el origen del ataque (supuestamente Corea del Norte).

Resultado: Se reforzó la seguridad digital en el sector del entretenimiento.

3. Caso Edward Snowden (EE. UU., 2013)

Resumen: Snowden filtró documentos clasificados de la NSA.

Aplicación forense: Se utilizó informática forense para rastrear cómo accedió a los datos, qué sistemas comprometió y qué documentos sustrajo.

Resultado: Cambios en políticas de vigilancia y debate global sobre privacidad.

Casos en España y América Latina

1. Caso Gescartera (España, 2001)

Resumen: Estafa financiera mediante una agencia de valores.

Aplicación forense: Se recuperó información de discos duros para rastrear operaciones fraudulentas.

Resultado: Condenas por estafa y falsedad documental.

2. Caso Bankia – Correos de Blesa (España, 2013)

Resumen: Investigaciones de corrupción y mala gestión bancaria.

Aplicación forense: Peritos accedieron a correos electrónicos eliminados de Miguel Blesa (expresidente de Caja Madrid).

Resultado: Apoyo en juicios por la salida a bolsa y tarjetas black.

3. Caso de espionaje político con Pegasus (México, 2017)

Resumen: Se reveló que el gobierno mexicano usó el software espía Pegasus para espiar a periodistas y activistas.

Aplicación forense: Laboratorios como Citizen Lab realizaron análisis forenses en los teléfonos afectados, encontrando rastros del software malicioso.

Resultado: Escándalo internacional y cuestionamiento sobre el uso de herramientas de vigilancia.

Tráfico de partes de jaguar: análisis genético forense

DELITO NACIONAL

La bióloga boliviana Paola Nogales ha liderado un proyecto innovador que utiliza técnicas de secuenciación genómica para rastrear el origen de partes de jaguares traficadas ilegalmente. Su trabajo ha permitido identificar rutas de caza y tráfico, así como establecer la existencia de dos poblaciones genéticas diferenciadas de jaguares en Bolivia. Sin embargo, ha enfrentado obstáculos legales para acceder a muestras decomisadas por las autoridades, lo que ha limitado el alcance de sus investigaciones.

Ejemplos de aplicación de la informática forense:

Investigación de delitos informáticos:

Se utiliza para investigar ciberataques, como el robo de identidad, la distribución de malware, o el acceso no autorizado a sistemas informáticos.

Análisis de redes:

Implica el monitoreo y análisis del tráfico de red para identificar actividades sospechosas, como intentos de piratería o filtraciones de datos.

Análisis de dispositivos móviles:

Permite la recuperación de datos de dispositivos móviles, como mensajes, llamadas y ubicaciones GPS, para fines forenses.

Recuperación de datos eliminados:

Se puede utilizar para recuperar archivos que han sido borrados accidental o deliberadamente, o que han sido dañados por un virus o malware.

Análisis de sistemas de archivo:

Implica el análisis de la estructura de archivos en un sistema operativo para identificar actividad sospechosa, como la creación o modificación de archivos en un momento inusual.

Análisis de memoria volátil:

Se utiliza para analizar el contenido de la memoria RAM de un sistema para identificar procesos activos, conexiones de red y otras pistas relevantes.

Análisis de correos electrónicos:

Permite analizar el contenido de correos electrónicos para identificar si son legítimos o forman parte de un ataque de phishing u otras estafas.

Análisis de bases de datos:

Implica el análisis de bases de datos para identificar datos que puedan ser relevantes para una investigación, como registros de acceso o actividad sospechosa.

Análisis de cloud:

Se utiliza para investigar incidentes de seguridad en entornos de nube, como la pérdida de datos o el acceso no autorizado.

Análisis de sistemas operativos:

Permite analizar el funcionamiento de un sistema operativo para identificar vulnerabilidades o actividad sospechosa.

Investigación de casos civiles y penales:

Se puede utilizar para recopilar pruebas digitales en casos civiles y penales, como disputas comerciales, robos o asesinatos.

Análisis de malware:

Se utiliza para identificar y analizar malware, como virus o troyanos, para comprender su funcionamiento y fuente.

Análisis de software:

Permite analizar el código de un software para identificar vulnerabilidades o backdoors.

Análisis de datos latentes o ambientales:

Implica la búsqueda de información que ha sido borrada o que no es visible a simple vista, pero que aún puede ser recuperada mediante técnicas forenses.

Análisis de red de dispositivos IoT:

Implica el análisis de dispositivos IoT para identificar vulnerabilidades y ataques.

Análisis de dispositivos de almacenamiento encriptados:

Permite la recuperación de datos de dispositivos encriptados.

Análisis de huellas digitales:

Implica el análisis de huellas digitales en dispositivos digitales, como teléfonos inteligentes, tablets y computadoras.

La informática forense en Bolivia es un campo muy importante para la investigación y resolución de delitos relacionados con la tecnología y la información digital. Aquí te explico de manera amigable cómo se opera y quiénes están involucrados

¿CÓMO SE OPERA LA INFORMÁTICA FORENSE EN BOLIVIA?

Recolección de evidencia digital: Los expertos en informática forense recopilan datos de computadoras, teléfonos, servidores y otros dispositivos electrónicos, asegurándose de no alterar la información original.

Análisis de la evidencia: Se analizan los datos para identificar actividades ilícitas, rastrear autores, recuperar información borrada y entender cómo ocurrió el delito.

Preservación de la evidencia: Es fundamental mantener la integridad de los datos para que puedan ser utilizados en procesos judiciales, siguiendo protocolos estrictos para evitar manipulaciones.

Informe y presentación: Los resultados del análisis se documentan claramente y se preparan informes que pueden ser utilizados en tribunales para sustentar las investigaciones.

¿Quiénes operan en informática forense en Bolivia?

Peritos y expertos en informática forense: Profesionales especializados en análisis digital, que trabajan en instituciones públicas, privadas o de manera independiente.

Fuerzas policiales y judiciales: La Policía Boliviana, especialmente unidades como la Fuerza Especial de Lucha Contra el Crimen (FELCC), cuentan con expertos en informática forense para apoyar en investigaciones criminales.

Ministerio Público: Los fiscales y abogados especializados en delitos informáticos utilizan los informes forenses para sustentar sus casos en los tribunales.

Instituciones académicas y de investigación: Algunas universidades en Bolivia ofrecen formación en informática forense y contribuyen con investigación y capacitación en el área.

Empresas privadas y consultoras: Firmas especializadas en seguridad digital y análisis forense que brindan servicios a empresas y organizaciones para protegerse contra delitos cibernéticos.

VI. MARCO TEORICO

Informática: La informática, también llamada computación, es el área de la ciencia que se encarga de estudiar la administración de métodos, técnicas y procesos con el fin de almacenar, procesar y transmitir información y datos en formato digital. La informática abarca desde disciplinas teóricas hasta disciplinas prácticas.

Forense: utiliza para describir las prácticas y técnicas aplicadas en el ámbito judicial

Cibercrimen: El cibercrimen, también conocido como ciberdelincuencia, se refiere a cualquier actividad delictiva que se realiza o se facilita a través de computadoras, redes informáticas o dispositivos en red. Incluye una amplia gama de delitos, desde robos de identidad y fraudes financieros hasta ataques a sistemas informáticos y ciberacoso.

Evidencia: Las evidencias son objetos o señales contrastados que permiten relacionar los elementos o hechos. Cuando se habla de evidencia se determina la certeza de una cosa. Pueden convertir a los indicios en argumentos científicos que confirman o descartan la hipótesis sobre la cual se trabajaba.

La base para la elaboración de los informes periciales está en las evidencias. Cuanto mayor sea el número de evidencias, mayor seguridad habrá en la verdad que se intenta comprobar. Habitualmente se confunden con las pruebas, pero no son lo mismo, aunque podrían convertirse en ellas.

Informática forense: La informática forense o computación forense es una rama de la ciberseguridad que se encarga de investigar delitos informáticos, tales como robo de información personal, brechas de seguridad informática en sistemas operativos, hackeo de dispositivos móviles, redes, correos electrónicos, discos duros, o ciberataques dirigidos a irrumpir en la seguridad de la red.

Software de análisis forense: El software de análisis forense es un conjunto de herramientas especializadas que se utilizan para investigar dispositivos digitales, permitiendo la recuperación, inspección y análisis de datos de computadoras, teléfonos inteligentes y tablets. Su objetivo principal es extraer, preservar, analizar

y presentar evidencias digitales para investigar crímenes cibernéticos, incidentes de seguridad y auditorías.

Análisis forense: El análisis forense, o análisis forense digital, es el proceso de recopilar, preservar y analizar pruebas digitales para investigar incidentes cibernéticos, delitos informáticos o cualquier otro evento que involucre datos electrónicos. Su objetivo es identificar y comprender lo que sucedió, quién estuvo involucrado y cómo sucedió, utilizando técnicas científicas y herramientas especializadas.

Seguridad informática: La seguridad de la tecnología de la información (seguridad informática) constituye un amplio conjunto de medidas multidisciplinares de protección para evitar que una red informática y sus datos sufran algún tipo de vulneración, filtración, publicación de información privada o ataque.

La seguridad informática es esencial para prevenir ataques e intentos de phishing, robo de información, vulneraciones de seguridad y destrucción de la propiedad. Cada vez existe un riesgo mayor para todo tipo de dispositivos, incluidos tablets y móviles, puesto que ahora estos aparatos almacenan más datos públicos y privados que la mayoría de ordenadores. Debido al crecimiento exponencial de los ciberataques durante el último año, la mayoría de empresas e individuos sufrirán interrupciones de su actividad y robo de datos.

Criptografía: La criptografía es un método de protección de la información y las comunicaciones mediante el uso de códigos que permite que solo aquellos a quienes está destinada la información puedan leerla y procesarla.

Los criptógrafos protegen los sistemas informáticos y de tecnología de la información mediante la creación de algoritmos y códigos para cifrar los datos. A menudo también llevan a cabo las tareas de un criptoanalista, descifrando algoritmos y descodificando texto para descifrar información.

Cadena de custodia: El proceso mediante el cual se registra el manejo de la evidencia para evitar su alteración.

Imagen forense: Copia exacta de los datos de un dispositivo, creada de manera que no altere la información original.

Hash: Función criptográfica que genera un valor único a partir de un archivo o conjunto de datos, utilizado para verificar su integridad.

Malware: Software diseñado para dañar o acceder sin permiso a sistemas informáticos.

Análisis de memoria: Estudio de la memoria RAM de un sistema para detectar rastros de actividad maliciosa.

Sleuth Kit: Conjunto de herramientas forenses utilizado para examinar discos y recuperar archivos eliminados.

VI. CONCLUSIONES

Este trabajo nos permite de alguna manera conocer la importancia de la Informática Forense ya que es una disciplina fundamental en el contexto actual, donde los delitos digitales están en aumento. Su capacidad para recuperar y presentar evidencia digital de manera válida y legalmente aceptada la convierte en un pilar esencial tanto en el ámbito judicial como en la seguridad corporativa. El proceso forense es riguroso, detallado y requiere un alto nivel de especialización y herramientas avanzadas para garantizar que la evidencia presentada sea auténtica y precisa.

De esta manera ayudar a la sociedad cuando estén expuestos a tantos fraudes, así también puede ayudar a las empresas mediante diversas pruebas técnicas, Al mismo tiempo se encargará de detectar estos fraudes, no crean, aunque esto no se termina esto crece día a día pues con un interfaz se nos presentan y cuando menos nos damos cuenta ya estamos adentro de un fraude

VII. RECOMENDACIONES

Se recomienda capacitar sobre el tema ya que es de mucha importancia conocer un poco respecto a la informática forense, hoy en día en cada país del mundo la tecnología va avanzando, los fraudes, las nueves por internet están aun mas en nuestros tiempos como la informática forense.

Los tribunales y las autoridades judiciales deben confiar en que la evidencia digital presentada sea real, respaldada sin ninguna manipulación. Para ello los expertos forenses deben seguir procedimientos estandarizados y presentar la videncia de manera transparente.

VIII. ANEXOS

IX. WEBGRAFIA

- https://www.deltaprotect.com/blog/informatica-forense-que-es#:~:text=La%20inform%C3%A1tica%20forense%20se%20encarga,%2C%20ataque%20DDoS%2C%20entre%20otros.
- https://msmk.university/que-es-la-informatica-forense-msmk-university/
- https://www.campusciberseguridad.com/blog/informatica-forense-herramientas-tecnicas-deber-dominar
- https://www.studocu.com/latam/document/universidad-autonoma-de-santo-domingo/introduccion-a-la-informatica/informatica-forense-informacion-de-informatica-forense/72634783
- Casey, E. (2011). Digital Evidence and Computer Crime. Academic Press.
- Nelson, B., Phillips, A., & Steuart, C. (2018). Guide to Computer Forensics and Investigations. Cengage Learning.
- Kruse, W. G., & Heiser, J. G. (2001). Computer Forensics: Incident Response
- https://www.laboratoriodeinformaticaforense.com/5-claves-para-entender-la-importancia-de-la-informatica-forense/