UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE CIENCIAS PURAS Y NATURALES

CARRERA DE INFORMATICA

TESIS DE GRADO

"ANALISIS INFORMATICO FORENSE PARA LA RECOPILACION CONFIABLE DE DATOS Y EVIDENCIAS DIGITALES"

PARA OPTAR AL TITULO DE LICENCIATURA EN INFORMÁTICA

MENCIÓN: INGENIERÍA DE SISTEMAS INFORMÁTICOS

Postulante	**:**	**Lizeth Rodríguez Rojas**
Tutor	**:**	**Lic. Efraín Silva Sánchez**
Revisor	**:**	**M. Sc. Carlos Mullisaca Choque**

La Paz – Bolivia
2011

DEDICATORIA

A Dios por permitirme seguir en los momentos más difíciles y no dejarme desfallecer.

A mis padres Carlos y Eva a quienes amo con todo mi ser, por las muestras de cariño, por apoyarme, corregirme y comprenderme.

A mis hermanos Maritza, Percy, William e Ivanna, por el cariño y apoyo incondicional que me brindan.

Lizeth Rodríguez Rojas

AGRADECIMIENTOS

Quiero agradecer a todas las personas que de una forma u otra han hecho posible esta tesis. La lista es larga y son muchos los que con sus consejos, escuchándome o dándome ánimos han contribuido a que este trabajo siguiera adelante.

A mis padres, Carlos y Eva, por apoyarme siempre en todo, por confiar en mí y por su enorme afecto. Gracias por haberme dado tanto, y por todo lo que se sacrifican día a día.

A toda mi familia: tíos, primos y sobrinos, por creer siempre en mí y por todas sus palabras de aliento.

De manera especial me gustaría dar las gracias:

A mi Tutor Lic. Efraín Silva Sánchez, por su confianza, guía y apoyo. Sin su empeño y conocimientos este trabajo no hubiese sido posible.

A mi Revisor MSc. Carlos Mullisaca Choque, por las sugerencias, correcciones y el tiempo dedicado a mi tesis, quien me brindó su apoyo constantemente para poder culminar el presente trabajo.

A todos los docentes de la Carrera de Informática, por brindarnos sus conocimientos de manera desinteresada y con dedicación, de quienes aprendí mucho y les estaré eternamente agradecida.

A la Universidad Mayor de San Andrés casa superior de estudios que durante este tiempo me albergo.

A mis amigos por todos esos momentos de aliento, por apoyarme, por aguantarme y por estar siempre ahí.

A todos, GRACIAS.

RESUMEN

En los últimos años en Bolivia ya se hacen presentes las investigaciones sobre posibles ilícitos donde se ven implicados elementos informáticos

Al ser la informática forense una disciplina que no tiene muchos años siendo practicada en nuestro medio, se cometen errores al momento de manejar la evidencia digital parte fundamental en investigaciones de éste tipo, lo cual resta credibilidad al ser tratada de manera inadecuada y por ende es vulnerable a ser inadmisible en un proceso penal.

Debido a lo explicado anteriormente, es que en la presente Tesis de Grado se desarrolla y propone un Método de análisis Informático Forense que permita la recopilación confiable de datos y evidencia digital, mantener de los elementos probatorios la autenticidad, confiabilidad, suficiencia y conformidad con la legislación vigente en nuestro país; estos cuatro conceptos son fundamentales para lograr que la evidencia sea admisible.

Para tal efecto se desarrollan procedimientos para la identificación, recopilación, preservación y análisis de la evidencia digital, además de un procedimiento para que la evidencia digital sea permitida legalmente, con la finalidad de precautelar la integridad de la misma y hacer que ésta sea aceptable en un proceso jurídico en nuestro país.

ABSTRACT

Of late years right now the gifts are made in Bolivia present the investigations on possible illicit acts where elements look implicated information-technology

To the being the forensic information technology a discipline that you do not have a lot of years being practiced in our means, commit him errors at the moment of managing the digital evidence the guy departs fundamental from in investigations this, which discredits the being treated of inadequate way and as a consequence it is vulnerable to be in a criminal action inadmissibly.

Due to what's explained previously, it is than in attendee The Tésis willingly he develops and a Method of Information-Technology Forensic analysis that the reliable compilation of data and digital evidence, to maintain allows to of the evidential elements proposes authenticity, reliability, sufficiency and conformity with the legislation in use at our country; These four concepts are fundamental to achieve that evidence is admissible.

For such effect procedures for the identification, compilation, preservation and analysis of the digital evidence, in addition to a procedure in order that the digital evidence is allowed to the same integrity of her, with the aim of pre-preventive legally and being done to that this is acceptable in a judicial process at our country develop.

I N D I C E

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

INDICE DE FIGURAS Y TABLAS

CAPITULO I

CAPITULO I

MARCO REFERENCIAL

1.1. INTRODUCCION

Cada día que pasa la informática forense adquiere gran importancia dentro de las tecnologías de información, debido al aumento del valor de la misma así como, la proliferación de redes y sistemas informáticos que han diversificado la forma en la que los delincuentes comenten los crímenes.

Es habitual encontrar nuevas amenazas para la seguridad informática, los delitos relacionados con la posesión, distribución, falsificación y fraude de información se realizan tras un escritorio, esto muestra un panorama complejo, en el cual los profesionales de las tecnologías de la información y los profesionales de la defensa de la ley deben cooperar y trabajar juntos en la defensa, detección y procesamiento de las personas que utilizan las nuevas tecnologías para realizar delitos informáticos.

En vista de que la mayoría de nosotros usamos las computadoras para comunicarnos, aprender, trabajar e inclusive para entretenimiento, llegamos a percibirlas como una extensión de nosotros mismos. Por esta razón, nuestras computadoras, en la mayoría de los casos, contienen información muy importante que puede ser usada como prueba o evidencia en procesos legales, tanto en materia penal como en civil, inclusive en el caso en que la evidencia no sea directamente relacionada con las computadoras.

En los últimos años en Bolivia ya se hacen presentes las investigaciones forenses debido al crecimiento de los delitos informáticos, la presente propuesta apoyaría de gran manera en el esclarecimiento de delitos cometidos bajo soporte informático, lo cual permite la solución de conflictos tecnológicos relacionados con seguridad informática y protección de datos.

Se suele definir el análisis forense, en su acepción más general, como la "*aplicación de la ciencia a cuestiones de interés legal*". En el contexto de Tecnología de la Información y la Seguridad de la Información, se define como "*la inspección sistemática y tecnológica de un sistema informático y sus contenidos para la obtención de evidencia de un crimen o cualquier otro uso que sea investigado*".

La informática forense, aplicando procedimientos estrictos y rigurosos puede ayudar a resolver grandes crímenes apoyándose en el método científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales.

En la presente investigación se facilitarán los pasos necesarios para atender de forma rápida, oportuna y confiable a cualquier incidente de seguridad y así proporcionar datos creíbles para posterior análisis a tomar en cuenta en el campo legal este tema como uno de los puntos claves para el buen funcionamiento de los equipos. En este momento, la seguridad no es un lujo. Es una necesidad.

1.2. ANTECEDENTES

La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.

Desde 1984, el Laboratorio del FBI y otras agencias que persiguen el cumplimiento de la ley empezaron a desarrollar programas para examinar evidencia computacional.

Actualmente el uso de metodologías, procedimientos y métodos de análisis forense de esta área, enfatizando el área de Computación forense es escaso, que

permitan realizar un manejo adecuado para que la evidencia digital sea confiable y también se aplique en nuestro medio.

En algunas publicaciones de revistas científicas dicen que en la informática forense se debe aplicar los métodos referentes a ésta, pero no dan a conocer en qué consisten esos métodos.

Por ejemplo en el artículo científico "Informática Forense" [Reino, 2007], indica que "*la metodología aplicada debe ser conocida, de forma que otros investigadores, utilizando los mismos métodos, puedan llegar a conclusiones similares*", pero realizando investigaciones no se tiene conocimiento de éstos métodos y mitologías a las que hace referencia el autor.

1.3. PLANTEAMIENTO DEL PROBLEMA

El análisis forense es una pieza clave en los procesos de respuesta a incidentes de seguridad, y sirve para establecer datos como el "qué", "quién", "cuándo", "cómo", y en algunos casos, el "por qué" de un incidente.

Actualmente existe la carencia parcial o total de un método que permita la investigación forense, para establecer adecuadamente, técnicamente y claramente, la acumulación de evidencias inobjetables destinadas al esclarecimiento de un problema ilícito para su posterior proceso legal.

1.4. PROBLEMA CENTRAL

¿Mediante el método de análisis informático forense se podrá obtener a través del tratamiento de la información pruebas electrónicas confiables, las mismas se pueden utilizar según la legislación boliviana como elemento probatorio de práctica ilícita?

1.5. HIPÓTESIS

El método de análisis informático forense optimiza la recopilación datos y evidencias digitales de manera confiable y eficiente, garantizando la admisibilidad coherente en contextos jurídicos d nuestro país.

1.6. OBJETIVOS

1.6.1. OBJETIVO GENERAL

Desarrollar y plantear un método de análisis informático forense, para obtener evidencias digitales confiables que garanticen la aceptación de la misma manteniendo la autenticidad, confiabilidad, suficiencia, conformidad con las leyes y reglas de justicia en nuestro país.

1.6.2. OBJETIVOS ESPECÍFICOS

- Realizar un estudio de las diferentes herramientas desarrolladas para el análisis informático forense.
- Plantear un procedimiento para la identificación de la evidencia digital.
- Plantear un procedimiento para la recopilación de la evidencia digital
- Plantear un procedimiento para preservar la evidencia digital
- Plantear un procedimiento para analizar la evidencia digital.
- Plantear un formato de reporte sobre las pruebas obtenidas.
- El método planteado facilite su mejor desempeño, a los seguidores de esta área.

1.7. JUSTIFICACION

1.7.1. JUSTIFICACION CIENTIFICA

Es factible el desarrollo del método de análisis informático forense pues se aplican en su diseño y su construcción herramientas aplicando el método científico.

1.7.2. JUSTIFICACION SOCIAL

El método de análisis informático forense será una herramienta importante, pues realiza un diagnostico legal que permita la presentación de evidencias digitales aceptables ante las instancias legales oportunas.

1.7.3. JUSTIFICACION ECONOMICA

Económicamente tiene un gran impacto, puesto que cuando se investiga delitos informáticos, en la mayoría de los casos se espera un resarcimiento de daños a las victimas dispuestos por la autoridad competente.

1.8. ALCANCES Y LIMITES

Se elaborará el método de análisis informático forense para la obtención confiable de evidencia digital, detallada y formal. Se explicará de la mejor manera la aplicabilidad del mismo, el cual brinda al informático contar con un material específico, que facilite emitir resultados con respecto a investigaciones realizadas, en delitos cometidos con soporte informático

El cual contará con procedimientos específicos para:

- Identificar la evidencia

- Preservar la evidencia digital
- Recopilar la evidencia digital
- Analizar la evidencia digital

Éste método de análisis informático forense está propuesto tomando en cuenta la perspectiva de ser aplicado en el campo de Computer forensics (computación forense) y no así en digital forensics (forensia digital) o network forensics (forensia en redes), que también son partes de la Informática Forense.

El método de análisis informático forense para la recopilación confiable de datos y evidencia digital, se encuadra sólo hasta que la prueba electrónica sea permitida en un proceso jurídico.

1.9. METODOLOGIA

La presente investigación es de tipo descriptivo por sus características así, estas se observan y se describen tal como se presentan en su ambiente natural. Su metodología es fundamentalmente descriptiva, aunque puede valerse de algunos elementos.

1.9.1 MÉTODO CIENTÍFICO

Este método científico se suele utilizar para mejorar o precisar teorías previas en función de nuevos conocimientos, donde la complejidad del modelo no permite formulaciones lógicas. Por lo tanto, tiene un carácter predominantemente intuitivo y necesita, no sólo para ser rechazado sino también para imponer su validez, la contrastación de sus conclusiones.

Esto supone la adquisición de nuevo conocimiento, mediante el estudio de evidencia observable y medible, aplicando el razonamiento lógico, elaborando modelos e hipótesis, y corrigiendo o mejorando estas últimas según se obtiene más evidencia.

La primera característica del método científico es su naturaleza convencional, la de servir de marco de generación del conocimiento objetivo. Por ello existen múltiples características en función de la perspectiva con que se clasifiquen, se estudien e incluso se denominen.

Además, los resultados deben ser objetivos e imparciales. La metodología aplicada debe ser conocida, de forma que otros investigadores, utilizando los mismos métodos, puedan llegar a conclusiones similares.

Los resultados de la investigación deben explicar de forma clara las relaciones de causa y efecto, eliminar en la medida de lo posible alternativas plausibles, y evitar las conclusiones no falsables. Que una afirmación sea falsable, significa que sería posible, al menos de forma teórica, demostrar su falsedad mediante la observación y descubrimiento de nueva evidencia.

Los estrictos requisitos del método científico no excluyen elementos de la experiencia humana como son las "corazonadas" y la intuición. Éstas son de gran utilidad a la hora de proponer hipótesis y modelos, que luego deben ser corroborados por la fría evidencia, de una forma estricta y objetiva.

CAPITULO II

CAPITULO II

MARCO TEÓRICO

2.1 INFORMÁTICA FORENSE

La informática forense está adquiriendo una gran importancia dentro del área de la información electrónica, esto debido al aumento del valor de la información y/o al uso que se le da a ésta, al desarrollo de nuevos espacios donde es usada como y al extenso uso de computadores por parte de las compañías de negocios tradicionales.

Es por esto que cuando se realiza un crimen, muchas veces la información queda almacenada en forma digital. Sin embargo, existe un gran problema, debido a que los computadores guardan la información de información forma tal que no puede ser recolectada o usada como prueba utilizando medios comunes, se deben utilizar mecanismos diferentes a los tradicionales. Es de aquí que surge el estudio de la computación forense como una ciencia relativamente nueva.

Resaltando su carácter científico, tiene sus fundamentos en las leyes de la física, de la electricidad y el magnetismo. Es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada.

2.2 MARCO REFERENCIAL

La informática forense se define como una rama de la informática que se encarga de recolectar y/o recopilar información valiosa desde sistemas informáticos (redes, ordenadores, soportes magnéticos, ópticos, etc.) con distintos fines, sirviendo de apoyo a otras disciplinas o actividades, como son las labores de criminalística e investigaciones.

Estas evidencias que permite descubrir diferentes datos sirven, por ejemplo, para condenar o absolver a algún imputado. La idea principal de este tipo de informática es colaborar con la criminalística [Restrepo, 2007].

Se reconoce a Dan Farmer y Wietese Venema, como los pioneros de la informática forense, actualmente Brian Carrier es probablemente uno de los expertos mundiales en el tema.

Esta rama tuvo su origen en 1984 cuando el FBI y otras agencias de Estados Unidos comenzaron a desarrollar programas para examinar evidencia computacional.

La Informática Forense recolecta y utiliza la evidencia digital para casos de delitos informáticos y para otro tipo de crímenes usando técnicas y tecnologías avanzadas. Un experto en informática forense utiliza estas técnicas para descubrir evidencia de un dispositivo de almacenaje electrónico. Los datos pueden ser de cualquier clase de dispositivo electrónico como discos duros, discos compactos, discos flexibles, cintas de respaldo, computadores portátiles, memorias extraíbles, archivos y correos electrónicos.

La mayoría de los usuarios piensan que al borrar un archivo se quitará totalmente la información del disco duro. En realidad se quita solamente el archivo de localización, pero el archivo real todavía queda en su computadora.
La Informática Forense se puede utilizar para descubrir un fraude, uso no autorizado de computadoras, una violación de políticas de compañías, historial de chats, archivos y navegación o cualquier otra forma de comunicaciones electrónicas.

2.3 MARCO CONCEPTUAL

2.3.1 DEFINICIONES

Existen múltiples definiciones para el análisis forense en informática y por ende varios términos para aproximarnos a este tema, dentro de los cuales se tienen: computación forense, digital forensics (forensia digital), network forensics (forensia en redes), entre otros. Este conjunto de términos puede generar confusión en los diferentes ambientes o escenarios donde se utilice, pues cada uno de ellos trata de manera particular.

2.3.2 CLASIFICACIÓN

Computer forensics, cuya traducción por lo general se hace como computación forense. Esta expresión podría interpretarse de dos maneras:

i) Disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso.

ii) Como la disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos.

Estas dos definiciones no son excluyentes, sino complementarias. Una de ellas hace énfasis en las consideraciones forenses y la otra en la especialidad técnica, pero en últimas ambas procuran el esclarecimiento e interpretación de la información en los medios informáticos como valor fundamental, uno para la justicia y otro para la informática.

Cuando se habla de network forensics, forensia en redes, estamos en un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular.

Esta conjunción de palabras establece un profesional que entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción.
A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, que en equipos particulares, es poco frecuente.

Digital forensics o forensia digital, trata de conjugar de manera amplia la nueva especialidad. Podríamos hacer semejanza con computación forense, al ser una forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos, de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática [Cano, 2003b].

2.3.3 DELITOS INFORMATICOS

Los delitos informáticos, en general, son aquellos actos delictivos realizados con el uso de computadoras o medios electrónicos, cuando tales conductas constituyen el único medio de comisión posible –o el considerablemente más

efectivo-, y los delitos en que se daña estos equipos, redes informáticas, o la información contenida en ellos, vulnerando bienes jurídicos protegidos [Wikipedia, 2008].

Existen dos Clasificaciones de Delitos Informáticos según Julio Téllez Valdés [Caracciolo]:

- Como instrumento o medio
- Como fin u objetivo

Todas aquellas conductas criminales que se valen de las computadoras como método, medio o símbolo para cometer un ilícito.

Como Instrumentos

Se utilizan a las computadoras para realizar falsificaciones de documentos de uso comercial. Tal es el caso de Recibos de Sueldos, Comprobantes, Escrituras.

Como Medios

Son conductas criminales en donde para realizar un delito utilizan una computadora como medio o símbolo.

Ejemplo de delitos Informáticos como instrumento o medio:

- Alteración de Documentación Legal.
- Planeamiento y simulación de delitos convencionales tales como robos, homicidios fraudes.
- Lectura, sustracción o copiado de información confidencial
- Modificación de datos tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria ficticia

- Uso no autorizado de programas.
- Introducción de instrucciones que provocan denegaciones de Servicios totales o parciales

Como Fin u Objetivos

Son conductas criminales que van dirigidas contra la computadora, sus accesorios o sus programas como entidad física. Es decir que son conductas criminales dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

Entre los delitos más habituales tenemos:

- ***Protección al menor***: producción, distribución y posesión de pornografía infantil.

- ***Fraude en las comunicaciones***: locutorios telefónicos clandestinos
  Dialers: modificación oculta del número de teléfono de destino, Producción y distribución de decodificadoras de televisión privada.

- ***Fraudes en Internet***: estafas, subastas ficticias y ventas fraudulentas.
  Carding: uso de tarjetas de crédito ajenas o fraudulentas. Phising: redirección mediante correo electrónico a falsas páginas simuladas trucadas (común en las mafias rusas).

- ***Seguridad lógica***: virus, ataques de denegación de servicio, sustracción de datos, hacking, descubrimiento y revelación de secretos, suplantación de personalidades, sustracción de cuentas de correo electrónico. Delitos de injurias, calumnias y amenazas a través del e-mail, news, foros, chats o SMS.

- ***Propiedad intelectual***: piratería de programas de ordenador, de música y de productos cinematográficos. Robos de código.

2.3.3.1. CASOS DETECTADOS EN BOLIVIA

Phishing

Los autores, quienes incluso operan desde otros países ingresan a la página web de alguna entidad financiera en la que escogen a su víctima; la contactan mediante su correo electrónico y le envían un portal falso del banco y bajo pretexto de que la institución está en un proceso de actualización le piden sus datos y el PIN.

Clonación de tarjetas

La víctima es afectada desde que asiste a un local o un centro comercial donde entrega su tarjeta de crédito para pagar sus compras o consumo, y el delincuente duplica su tarjera en un escáner sofisticado y se dan modos para seguirla y averiguar su clave, con la que después vacían su cuenta.

Sabotaje informático

Esta modalidad de fraude sucede cuando alguna persona, que puede ser ingeniero en sistemas, informático o conocedor de la internet, de forma maliciosa obstaculiza, modifica o comete cualquier otra acción que atente contra el normal funcionamiento de un sistema de información personal o de una institución.

Falsedad y amenazas

La falsificación y suplantación de identidad electrónica todavía no está en la legislación boliviana, pero consiste en que cierta persona averigua la contraseña de un correo electrónico ajeno y una vez que consigue ingresar modifica el contenido de cartas o documentos, o envía mensajes con diferentes fines a destinatarios.

2.3.4 DELINCUENCIA Y CRIMINALIDAD INFORMÁTICA

Es preciso que se reconozca la diferencia entre la criminología y la criminalística; La criminología trata de investigar el por qué y que fue lo que llevo al individuo a cometer el delito, mientras que la criminalística según Montiel Sosa , se definen como "una ciencia multidisciplinaria que reúne conocimientos generales, sistemáticamente ordenados, verificables y experimentables, a fin de estudiar, explicar y predecir el cómo, dónde, cuándo, quién o quienes los cometen" , la criminalística al ser multidisciplinaria se aplica en temas de balística, medicina forense, física, química, e incluso la informática, entre otras, y se apoya de métodos y técnicas propias del trabajo de las diferentes disciplinas.

Conocer el comportamiento de cómo los incidentes de seguridad, las vulnerabilidades y la criminalidad informática, es vital para el análisis de los delitos informáticos, ya que han tenido un repunte a los largo de los últimos años, por ello, se requiere analizar la tendencia de dichos componentes.

El informe de Evolución de Incidentes de Seguridad que corresponde al año 2007, elaborado anualmente desde 1999 por Red IRIS, determina que el incremento de incidentes que ha habido entre el año 2006 y 2007 es el 63.32% en el que se involucran escaneo de puertos en busca de equipos vulnerables, vulnerabilidades de sistemas web, errores de programación, vulnerabilidades de navegadores más utilizados, ataques de Phising, máquinas zombis, malware y otro tipo de ataques para el cometimiento de fraudes u inhabilitación de servicios, este mismo informe indica que el patrón de ataque continua siendo más dirigido, inteligente y silencioso con algún tipo de trasfondo que puede ser económico, religiosos, político o de ansias de poder. (Ver Figura: 1)

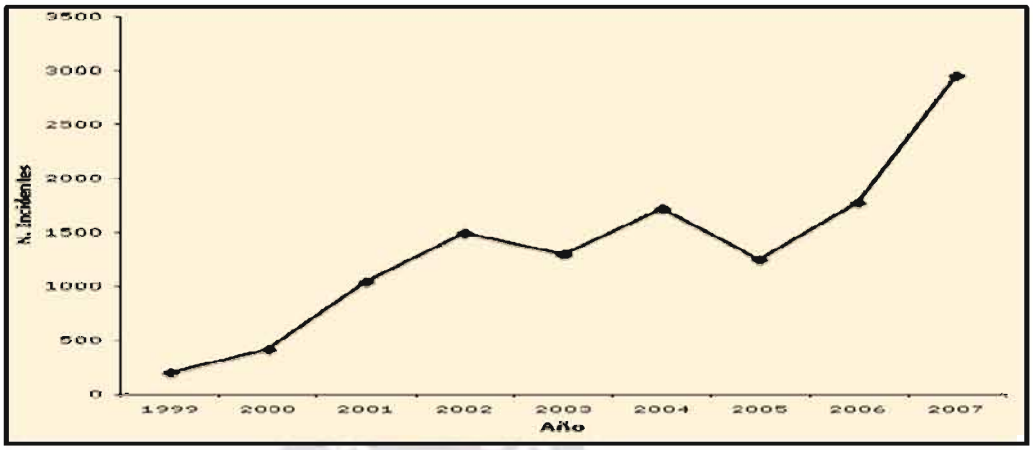


Figura. 1: Evolución de incidentes de seguridad

Fuente: REDIRIS – Informe de Evolución de Incidentes de Seguridad 2007.

Otro organismo que realiza investigaciones de este nivel es el CERT , que publica una variedad de estadísticas relacionadas con las vulnerabilidades, que se han catalogado basados en informes de fuentes públicas y reportes que son directamente comunicados mediante su sistemas web. Tal como se puede observar, se concluye que la tendencia sobre las vulnerabilidades tiene un crecimiento significativo a lo largo de los años que se han analizado (Ver Figura: 2).

Figura 2: Estadísticas de Vulnerabilidades

Fuente: CERT – Informe de vulnerabilidades reportadas 2007

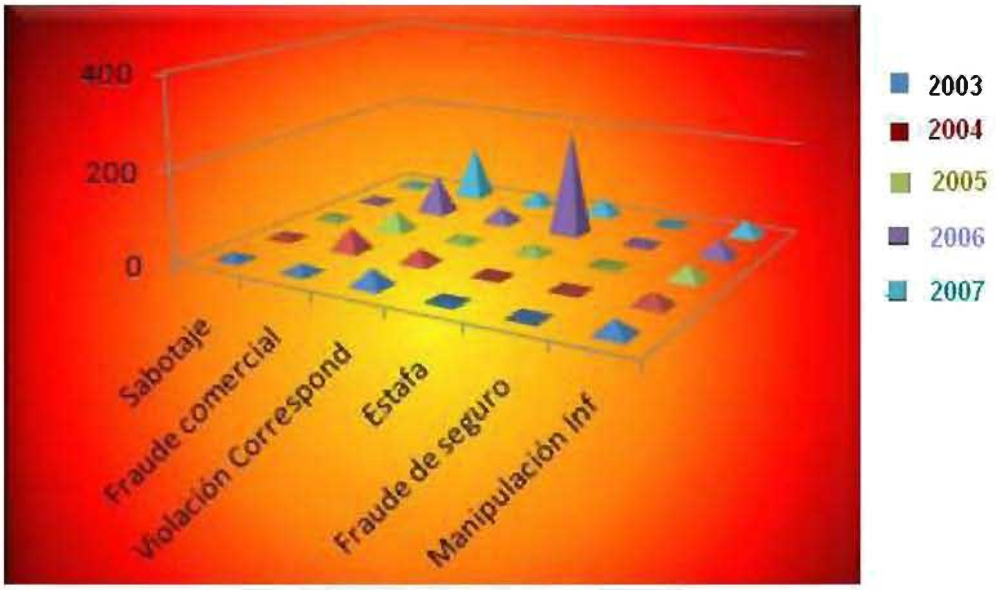


Figura 3: Casos Registrados en Bolivia

Fuente: FELCC

Los datos de la Fuerza Especial de Lucha Contra el Crimen (FELCC) revelan que en Santa Cruz, La Paz y Cochabamba se producen más delitos informáticos desde 2003.

Desde ese año hasta 2007, la Policía registró un total de 185 fraudes electrónicos en todo el país, de éstos, 177 corresponden a manipulación informática y ocho a alteración, acceso y uso indebido de información. De la primera figura legal, 91 casos hubo en Santa Cruz, 46 en Cochabamba, 30 en La Paz, cuatro en Potosí, tres en Oruro, dos en Beni y uno en Tarija.

Sobre alteración informática, tres ocurrieron en La Paz, dos en Cochabamba, dos en Beni y uno en Santa Cruz. Entre enero y septiembre de este año hubo 50 denuncias de manipulación electrónica (27 en Santa Cruz, 12 en La Paz, nueve en Cochabamba y dos en Chuquisaca) y ninguna acerca de alteración.

2.3.5 EVIDENCIA DIGITAL

Casey define la evidencia de digital como "cualquier dato que puede establecer que un crimen se ha ejecutado (commit) o puede proporcionar una enlace (link) entre un crimen y su víctima o un crimen y su autor". [Casey04]

"Cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático" [HBIT03]

A diferencia de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único de la evidencia computacional es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia. [ComEvi02].

Esta situación crea problemas concernientes a la investigación del robo de secretos comerciales, como listas de clientes, material de investigación, archivos de diseño asistidos por computador, fórmulas y software propietario.

Debe tenerse en cuenta que los datos digitales adquiridos de copias no se deben alterar de los originales del disco, porque esto invalidaría la evidencia; por esto los investigadores deben revisar con frecuencia que sus copias sean exactas a las del disco del sospechoso, para esto se utilizan varias tecnologías, como por ejemplo checksums o hash MD5 [DaVa01].

Cuando ha sucedido un incidente, generalmente, las personas involucradas en el crimen intentan manipular y alterar la evidencia digital, tratando de borrar cualquier rastro que pueda dar muestras del daño. Sin embargo, este problema es mitigado con algunas características que posee la evidencia digital. [Casey04]

• La evidencia de Digital puede ser duplicada de forma exacta y se puede sacar una copia para ser examinada como si fuera la original. Esto se hace comúnmente para no manejar los originales y evitar el riesgo de dañarlos.

• Actualmente, con las herramientas existentes, es muy fácil comparar la evidencia digital con su original, y determinar si la evidencia digital ha sido alterada.

• La evidencia de Digital es muy difícil de eliminar. Aun cuando un registro es borrado del disco duro del computador, y éste ha sido formateado, es posible recuperarlo.

• Cuando los individuos involucrados en un crimen tratan de destruir la evidencia, existen copias que permanecen en otros sitios.

2.3.5.1 CARACTERÍSTICAS DE LA EVIDENCIA DIGITAL

La evidencia digital posee las siguientes características:

1. Volátil
2. Anónima
3. Duplicable
4. Alterable y modificable
5. Eliminable

Estas características hacen de la evidencia digital un constante desafío para la identificación y el análisis, que exige al grupo de seguridad y auditoria la capacitación tanto en procedimientos, como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia en una escena del delito. Antes de realizar el proceso de análisis forense el equipo de seguridad o auditoría debe considerar los siguientes elementos para mantener la idoneidad del procedimiento forense.

- ✓ Evidencia altamente volátil

CPU (Registros, Caché), Memoria de Video. Usualmente la información en estos dispositivos es de mínima utilidad, pero debe ser capturada como parte de la imagen de la memoria del sistema.

✓ Evidencia medianamente volátil

La memoria RAM, incluye información sobre los procesos en ejecución, el hecho de capturarla hace que cambie. Requiere conocimiento especializado para poder reconstruirla, pero no se requiere mucho conocimiento para hacer una búsqueda de palabras clave. Tablas del Kernel (Procesos en ejecución), permiten analizar los procesos que pueden ser evidencia de actividades no autorizadas.

✓ Evidencia poco volátil

Medios Fijos (Discos Duros), Incluye área de swap, colas, directorios temporales, directorios de registros. La información recolectada en el área de swap y las colas permite analizar los procesos y la información de los mismos en un punto del tiempo en particular. Los directorios permiten reconstruir eventos.

2.3.6 ADMISIBILIDAD DE LA EVIDENCIA DIGITAL [Cano, 2003a]

La evidencia digital (representada en todas las formas de registro magnético u óptico generadas por las organizaciones) debe avanzar hacia una estrategia de formalización que ofrezca un cuerpo formal de evaluación y análisis que deba ser observado por el ordenamiento judicial de un país. En general, las legislaciones y las instituciones de justicia han fundado sus reflexiones sobre la admisibilidad de la evidencia en cuatro conceptos [Sommer, 1995][Casey, 2001][IOCE, 2000 cap.6], que a continuación se detallan.

2.3.6.1. AUTENTICIDAD

Sugiere ilustrar a las partes que la evidencia ha sido generada y registrada en los sitios relacionados con el caso, particularmente en la escena del posible ilícito o lugares establecidos en la diligencia de levantamiento de evidencia.

Asimismo, la autenticidad es entendida como aquella característica que muestra la no alterabilidad de los medios originales y busca confirmar que los registros aportados correspondan a la realidad evidenciada en la fase de identificación y recolección.

En los medios digitales, dada la volatilidad y alta capacidad de manipulación que se presenta en el almacenamiento electrónico. Si bien estas características también son, de alguna manera, inherentes a las vías tradicionales, el detalle se encuentra en que existe una serie de procedimientos asociados con el manejo y control de los mismos en las organizaciones, mientras que para los registros magnéticos aún no se tiene la misma formalidad.

Verificar la autenticidad de los registros digitales requiere, de manera complementaria, a la directriz general establecida por la organización sobre éstos, el desarrollo y configuración de mecanismos de control de integridad de archivos, es decir, necesita que una arquitectura exhiba mecanismos que aseguren la integridad de los registros y el control de cambios de los mismos.

Al establecer una arquitectura de cómputo con la que se fortalezca la protección de los medios digitales de registro y el procedimiento asociado para su verificación, aumenta sustancialmente la veracidad de las pruebas recolectadas y aportadas. En consecuencia, la información que se identifique en una arquitectura con estas características tendrá mayor fuerza y solidez, no sólo por lo que su contenido ofrezca, sino por las condiciones de generación, control y revisión de los registros electrónicos.

En otras palabras, al contar con mecanismos y procedimientos de control de integridad, se disminuye la incertidumbre sobre la manipulación no autorizada de la evidencia aportada y se concentra el proceso en los hechos y no en errores técnicos de control de la evidencia digital bajo análisis.

2.3.6.2. CONFIABILIDAD

Es otro factor relevante para asegurar la admisibilidad de la misma. La confiabilidad nos dice si, efectivamente, los elementos probatorios aportados vienen de fuentes que son creíbles y verificables y que sustentan elementos de la defensa o del fiscal en el proceso que se sigue. En medios digitales podríamos relacionar este concepto a ¿cómo se recogen y analizan las evidencias digitales?, son preguntas cuyas respuestas buscan demostrar que poseen una manera confiable para ser identificados, recopilados y verificados.

Cuando logramos que una arquitectura de cómputo ofrezca mecanismos de sincronización de eventos y una centralización de registros de sus actividades (los cuales, de manera complementaria, soportan estrategias de control de integridad), hemos avanzado en la formalización de la confiabilidad de la evidencia digital.

Asimismo, en el desarrollo de software o diseño de programas es necesario incluir, desde las primeras fases de la creación de aplicaciones, un momento para la configuración de logs o registros de auditoría del sistema ya que, de no hacerlo, se corre el riesgo de perder trazabilidad[1] de las acciones de los usuarios en el sistema y, por tanto, crear un terreno fértil para la ocurrencia de acciones no autorizadas, es decir, se sugiere que la confiabilidad de la evidencia en una arquitectura de cómputo estará en función de la manera como se sincronice la inscripción de las acciones de los usuarios y de un registro centralizado e íntegro de los mismos. Esto reitera la necesidad de un control de integridad de los registros del sistema para mantener su autenticidad.

2.3.6.3. SUFICIENCIA

Es la presencia de toda la evidencia necesaria para adelantar el caso; esta característica, al igual que las anteriores, es factor crítico de éxito en las investigaciones en procesos judiciales. Con frecuencia, la falta de pruebas o insuficiencia de elementos probatorios ocasiona la dilación o terminación de

[1] Trazabilidad - Capacidad de seguimiento y reconstrucción de acciones efectuadas por los usuarios en un sistema

procesos que podrían haberse resuelto. En este sentido, los abogados reconocen que, mientras mayores fuentes de análisis y pruebas se tengan, habrá más posibilidades de avanzar en la defensa o acusación en un proceso judicial.

Desarrollar estas particularidades en arquitecturas de cómputo requiere afianzar y manejar destrezas de correlación de eventos en registros de auditoría, es decir, si se cuenta con una arquitectura con mecanismos de integridad, sincronización y centralización, es posible establecer patrones de análisis que muestren la imagen completa de la situación bajo revisión.

La correlación de hechos (definida como el establecimiento de relaciones coherentes y consistentes entre diferentes fuentes de datos para establecer y conocer eventos ocurridos en una arquitectura o proceso) sugiere una manera de probar y verificar la suficiencia de los datos entregados en un juicio.

Si analizamos esta posibilidad, es viable establecer relaciones entre los datos y los sucesos presentados, canalizando las inquietudes y afirmaciones de las partes sobre comportamientos y acciones de los involucrados, sustentando dichas conexiones con acontecimientos o registros que previamente han sido asegurados y sincronizados.

Con esto en mente, la correlación se convierte en factor aglutinante de las características anteriores referenciadas para integridad y confiabilidad de la evidencia, lo que propone un panorama básico requerido en las arquitecturas de cómputo para validar las condiciones solicitadas por la ley en relación con las pruebas.

Es decir, que la correlación de sucesos (como una función entre la centralización del registro de eventos y el debido control de integridad de los mismos) se soporta en una sincronización formal de tiempo y eventos que deben estar disponibles por la arquitectura de cómputo para asegurar la suficiencia del análisis de la información presente en una arquitectura de cómputo.

2.3.6.4. CONFORMIDAD CON LAS LEYES Y REGLAS DE LA ADMINISTRACIÓN DE JUSTICIA

Hace referencia a los procedimientos internacionalmente aceptados para recolección, aseguramiento, análisis y reporte de la evidencia digital. Si bien están previstos en el código de procedimiento penal las actividades mínimas requeridas para aportar evidencia a los procesos, existen en medios digitales iniciativas internacionales donde se establecen lineamientos de acción y parámetros que cobijan el tratamiento de la evidencia en medios electrónicos, los cuales deben ser revisados y analizados en cada uno de los contextos nacionales para su posible incorporación.

2.3.7. DETERMINAR LA RELEVANCIA DE LA EVIDENCIA

El estándar en esta fase establece valorar las evidencias de tal manera que se identifiquen las mejores evidencias que permitan presentar de manera clara y eficaz los elementos que se desean aportar en el proceso y en el juicio que se lleve. El objetivo es que el ente que valore las pruebas aportadas observe en sus análisis y aportes los objetos de prueba más relevantes para el esclarecimiento de los hechos en discusión.

En este sentido el estándar sugiere dos criterios para tener en cuenta a saber:

a. Valor probatorio: que establece aquel registro electrónico que tenga signo distintivo de autoría, autenticidad y que sea fruto de la correcta operación, confiabilidad del sistema.

b. Reglas de la evidencia: que establece que se han seguido los procedimientos, reglas establecidas para la adecuada recolección y manejo de la evidencia.

2.4 MARCO JURIDICO

2.4.1. LEGISLACIÓN BOLIVIANA

En Bolivia, en el año de 1989, se consideró el análisis y tratamiento sobre Legislación Informática concerniente a contratación de bienes y servicios informáticos, flujo de información computarizada, modemización de aparato productivo nacional mediante la investigación científico- tecnológica en el país y la incorporación de nuevos delitos emergentes del uso y abuso de la informática.

Este conjunto de acciones tendientes a desarrollar de manera integral la informática, se tradujo en el trabajo de especialistas y sectores involucrados, representantes en el campo industrial, profesionales abogados y especialistas informáticos, iniciándose la elaboración de Proyecto de Ley Nacional de Informática, concluido en febrero de 1991.

Asimismo, el Código Penal Boliviano, texto ordenado según ley No 1768 de 1997, incorpora en el Título X un capítulo destinado a los Delitos Informáticos. Ambos cuerpos legales tratan de manera general los nuevos delitos emergentes del uso de la informática.

La Ley No 1768, no obstante de no estar exenta de la problemática actual, al abordar en el Capítulo XI la tipificación y penalización de delitos informáticos, no contempla la descripción de estas conductas delictivas detalladas anteriormente.

Por consiguiente, la atipicidad de las mismas en nuestro ordenamiento jurídico penal vigente imposibilita una calificación jurídico-legal que individualice a la mismas, llegando a existir una alta cifra de criminalidad e impunidad, haciéndose imposible sancionar como delitos, hechos no descriptos en la legislación penal con motivo de una extensión extralegal del ilícito penal ya que se estaría violando el principio de legalidad expreso en la máxima "Nullum crime sine lege" Así mismo resulta imposible extender el concepto de bienes muebles e inmuebles a bienes incorporales como ser los datos, programas e información computarizada.

Delitos Informáticos

Artículo 363.- Bis (manipulación informática). El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de un tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

Artículo 363.- Ter (Alteración acceso y uso indebido de datos informáticos). El que sin estar autorizado apoderare, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días."[Código Penal, 1999].

2.5 MARCO TECNOLÓGICO

2.5.1 HERRAMIENTAS FORENSES

Hablar de informática forense sin revisar algunas ideas sobre herramientas es hablar en un contexto teórico de procedimientos y formalidades legales.

Las herramientas informáticas, son la base esencial de los análisis de las evidencias digitales en los medios informáticos. Sin embargo, es preciso comentar que éstas requieren de una formalidad adicional que permita validar tanto la confiabilidad de los resultados de la aplicación de las mismas, como la formación y conocimiento del equipo de seguridad que las utiliza. Estos dos elementos hacen del uso de las herramientas, una constante reflexión y cuestionamiento por parte de la comunidad científica y práctica de la informática forense en el mundo.

Dentro de las herramientas frecuentemente utilizadas en procedimientos forenses en informática detallamos algunas para conocimiento general, que son

aplicaciones que tratan de cubrir todo el proceso en la investigación forense en informática (ver anexo B):

- ***ENCASE*** [2]
- ***FORENSIC TOOLKIT***[3]
- ***WINHEX***[4]

Si bien las herramientas detalladas anteriormente son licenciadas y sus precios oscilan entre los 600 y los 5000 dólares, existen otras que no cuentan con tanto reconocimiento internacional en procesos legales, que generalmente son aplicaciones en software de código abierto

2.5.2 CONFIABLIIDAD DE LAS HERRAMIENTAS FORENSES EN INFORMATICA

Para la computación Forense, otro reto emergente son las herramientas tecnológicas que los investigadores utilizan para adelantar sus pericias. Por un lado las herramientas con licenciadas, propiedad de firmas desarrolladoras de software para forensia digital, establecen un nicho de negocio que exige de los informáticos forenses en informática una importante inversión, tanto en hardware y software, para darles mayor formalidad y certeza a las partes involucradas en un caso de la evidencia digital.

Dichas inversiones no solo son en la adquisición, sino en el mantenimiento y la actualización de las mismas, lo que hace que los especialistas forenses deben constantemente reforzar sus habilidades en el uso de estos programas y mantenerse notificados de posibles errores, propios de las mismas y sus maneras de mitigarlos pues saben que un caso basado en la confiabilidad de las mismas se puede o no decidir.

---

[2] http //www encase com/products/ef_index asp

[3] http //www accessdata com/products/utk/

[4] http //www x-ways net/forensics/index-m html

De otra parte se encuentran las herramientas forenses de código abierto o también llamadas software libre, las cuales aún no cuestionadas en tribunales y poco se recomiendan como herramientas de uso formal para presentar en audiencias, por su condición de herramientas revisadas y analizadas por una comunidad de la cual poco se conoce de sus pruebas, de las personas que adelantan las mismas, ni el control de los errores.

Sin embargo otra corriente defiende estas herramientas frente a las licenciadas, diciendo que el mundo de código abierto todo está para la investigación de un tercero, que las pruebas se pueden adelantar con mayor confianza que en las abiertas, y que el nivel de confiabilidad es mayor, dado que son muchos "ojos" los que están tratando de mejorarla.

	LICENCIA	IMAGEN	CONTROL INTEGRIDAD	ANÁLISIS	ADMON CASO
ENCASE	si	si	si	si	si
FORENSIC TOOLKIT	si	si	si	si	si
WINHEX (Forensic edition)	si	si	si	si	si

Tabla 2: Herramientas Forenses con Licencia

Mientras esta disyuntiva continua, se adelantas importantes esfuerzos formales para probar las herramientas forenses como el proyecto de *National Institute of Standars and Tecnology* norteamiericano NITS cuyo objetivo es establecer una metodología para probar aplicaciones forenses en informática a travez de la especificación general de herramientas.

En este contexto, las pruebas que realicen a los programas y dispositivos de hardware serán útiles para dar cumplimiento a las exigencias propias del *test*

de Daubert[5] prueba de referencia generalizada para establecer la confiabilidad de las herramientas en computación forense.

En este sentido, los programas o las herramientas de computación forense requieren estudios y análisis detallados para contar con un nivel de aceptación de los mismos.

2.6 MARCO METODOLÓGICO

2.6.1 MÉTODO CIENTÍFICO

Este método científico se suele utilizar para mejorar o precisar teorías previas en función de nuevos conocimientos, donde la complejidad del modelo no permite formulaciones lógicas. Por lo tanto, tiene un carácter predominantemente intuitivo y necesita, no sólo para ser rechazado sino también para imponer su validez, la contrastación de sus conclusiones.

Se podría proponer, para estas tres variantes del método científico, la denominación de método deductivo, método intuitivo y método experimental o método de contrastación, o cualquier conjunto de palabras que hagan referencia a sus diferencias fundamentales y no planteen problemas a la memoria lingüística. En esta misma línea se encuentra la denominación de método lógico deductivo que a veces recibe el método deductivo.

La primera característica del método científico es su naturaleza convencional, la de servir de marco de generación del conocimiento objetivo. Por ello existen múltiples características en función de la perspectiva con que se clasifiquen, se estudien e incluso se denominen.

Una característica de ambos métodos es que pueden ir de lo general a lo particular o viceversa, en un sentido o en el inverso. Ambos utilizan la lógica y

[5] El test de Daubert es un conjunto de reglas extraídas de la sentencia de la Corte suprema de Justicia Estadounidense

llegan a una conclusión. En última instancia, siempre tienen elementos filosóficos subyacentes.

Ambos suelen ser susceptibles de contrastación empírica. Aunque el método deductivo es más propio de las ciencias formales y el inductivo de las ciencias empíricas, nada impide la aplicación indistinta de un método científico u otro a una teoría concreta.

La diferencia fundamental entre el método deductivo y el método inductivo es que el primero aspira a demostrar, mediante la lógica pura, la conclusión en su totalidad a partir de unas premisas, de manera que se garantiza la veracidad de las conclusiones, si no se invalida la lógica aplicada. Se trata del modelo axiomático propuesto por Aristóteles como el método científico ideal.

Por el contrario, el método inductivo crea leyes a partir de la observación de los hechos, mediante la generalización del comportamiento observado; en realidad, lo que realiza es una especie de generalización, sin que por medio de la lógica pueda conseguir una demostración de las citadas leyes o conjunto de conclusiones.

Dichas conclusiones podrían ser falsas y, al mismo tiempo, la aplicación parcial efectuada de la lógica podría mantener su validez; por eso, el método inductivo necesita una condición adicional, su aplicación se considera válida mientras no se encuentre ningún caso que no cumpla el modelo propuesto.

El método hipotético-deductivo o de contrastación de hipótesis no plantea, en principio, problema alguno, puesto que su validez depende de los resultados de la propia contrastación.

La Teoría General de la Evolución Condicionada de la Vida sería, en principio, una teoría basada en el método hipotético-deductivo o método de contrastación de hipótesis.

La teoría de Darwin, por el contrario, estaría encuadrada en el método inductivo; pero que a pesar de encontrar ejemplos contrarios no se invalida sino que se adecua para cuadrar cualquier triángulo.

2.6.2 RAZONAMIENTO DEDUCTIVO VÁLIDO [Rojo, 1996]

Llamamos razonamiento a un par ordenado ({**Pi**}: **q**)

Siendo **{Pi}** un conjunto finito de proposiciones, llamadas premisas

q una proposición llamada conclusión. Respecto de la cual se afirma que deriva de las premisas.

Un razonamiento es deductivo si y sólo si las premisas son evidencias de la verdad de la conclusión, es decir, si P1, P2, P3,..... Pn son verdaderas entonces q verdadera.

Un razonamiento deductivo es válido si no es posible que las premisas sean verdaderas y la conclusión falsa. De un razonamiento no se dice que es verdadero o falso, sino que es válido o no.

Llamamos regla de inferencia, a todo esquema válido de razonamiento, independientemente de la V o F de las proposiciones componentes. De éste modo toda regla de inferencia es tautológica. Un razonamiento deductivo es válido cuando el condicional cuyo antecedente es la conjunción de las premisas, y el consecuente es la conclusión, es tautológico. Son ejemplos de reglas de inferencia:

a) Ley del Modus Ponens:

$$\frac{\begin{array}{l} p \\ p \rightarrow q \end{array}}{q}$$

La notación clásica es SI p y p → q, ENTONCES q

b) Ley del Modus Tolens:

$$\begin{array}{l} p \rightarrow q \\ \sim q \\ \hline \sim p \end{array}$$

Este esquema es la notación clásica del condicional [(p →q) ^ ~q] → ~p

c) Ley del silogismo hipotético:

$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline p \rightarrow r \end{array}$$

Es decir, la proposición [(p →q) ^ (q →r)] → (p →r) es una tautología.

En cambio, el condicional [(p →q) ^ q] → p no es una forma validada de razonamiento, ya que la correspondiente tabla de valores de verdad nos muestra que no es tautológico.

2.6.3 MÉTODO INDUCTIVO

El método inductivo se conoce como experimental y sus pasos son:

Observación, Formulación de hipótesis, Verificación, Tesis, Ley y Teoría.

La teoría de la falsación funciona con el método inductivo, por lo que las conclusiones inductivas sólo pueden ser absolutas cuando el grupo a que se refieran sea pequeño: por ejemplo si uno advierte que los alumnos de pelo rizado de un grupo escolar lograron en ortografía calificaciones superiores a las del promedio, una conclusión legitima será que todos los morenos de ese grupo muestran calificaciones superiores a las del promedio. Pero no es legítimo extraer

conclusiones acerca de las calificaciones de los pelirrojos en otros grupos ni en grupos futuros [Dávila, 2006].

El método inductivo crea leyes a partir de la observación de los hechos, mediante la generalización del comportamiento observado; en realidad, lo que realiza es una especie de generalización, sin que por medio de la lógica pueda conseguir una demostración de las citadas leyes o conjunto de conclusiones.

Dichas conclusiones podrían ser falsas y, al mismo tiempo, la aplicación parcial efectuada de la lógica podría mantener su validez; por eso, el método inductivo necesita una condición adicional, su aplicación se considera válida mientras no se encuentre ningún caso que no cumpla el modelo propuesto.

CAPITULO III

CAPITULO III

MARCO APLICATIVO

La evidencia digital es muy frágil y puede perderse o modificarse con demasiada facilidad, un mal manejo de la misma produce una disminución de la credibilidad que se tenía sobre ésta y una posible impunidad, al ser anuladas o inadmisibles en un juicio.

Esa evidencia digital será utilizada para descubrir o formar los elementos del delito o descubrir la identidad del sujeto activo, y luego, en su caso aportar la misma al proceso penal a fin de poder obtener la condena del mismo, sin sufrir las consecuencias de la nulidad de las pruebas o la inadmisibilidad de éstas en el juicio.

Para que la evidencia digital pueda garantizar la recopilación confiable y esta sea admisible en un proceso jurídico en nuestro país, se debe seguir los siguientes procedimientos:

Figura 4: Método de Análisis Informático Forense
Fuente: Elaboración propia

3.1. FASE DE IDENTIFICACIÓN

En ésta primera fase se debe asegurar la integridad de la evidencia original, es decir, que no se deben realizar modificaciones ni alteraciones sobre dicha evidencia, en este aspecto tratar de mantener los requerimientos legales.
Adicionalmente, es preciso que el investigador o especialista se cuestione sobre la información obtenida en un sistema que se crea está comprometido.

Aquí se pregunta:

- ✓ ¿Qué información se necesita?
- ✓ ¿Cómo aprovechar la información presentada?
- ✓ ¿En qué orden ubico la información?
- ✓ ¿Acciones necesarias a seguir para el análisis forense?

La identificación debe prever los desafíos que se pasaran durante los procesos de las fases de preservación y extracción. Esta fase culmina con un Plan a seguir.

3.1.1. SOLICITUD FORENSE

La solicitud forense es un documento donde el administrador del equipo afectado notifica de la ejecución de un incidente y para ello solicita al equipo de seguridad la revisión del mismo, donde incluye toda la información necesaria para dar inicio al proceso de análisis. La información incluida en el documento debe ser la siguiente:

- ➢ DESCRIPCIÓN DEL DELITO INFORMÁTICO
  - ➢ Fecha del incidente
  - ➢ Duración del incidente

- Detalles del incidente

- INFORMACIÓN GENERAL
  - Área
  - Nombre de la dependencia
  - Responsable del sistema afectado
    - Nombres y Apellidos
    - Cargo
    - E-mail
    - Teléfono
    - Extensión
    - Celular
    - Fax

- INFORMACIÓN SOBRE EL EQUIPO AFECTADO
  - Dirección IP
  - Nombre del equipo
  - Marca y modelo
  - Capacidad de la RAM
  - Capacidad del disco duro
  - Modelo del procesador
  - Sistema operativo (nombre y versión)
  - Función del equipo
  - Tipo de información procesada por el equipo

- ✓ Toda la información del incidente, la evidencia digital, copias o imágenes de la escena del crimen.

METODO ANÁLISIS INFORMÁTICO FORENSE

1. DESCRIPCIÓN DEL DELITO INFORMÁTICO

Fecha del incidente: _____

Si se puede establecer, ¿cuál fue la duración del incidente?_____

En pocas palabras, enumere los detalles del incidente

¿Cómo se descubrió el incidente?

_____

_____

Si es posible realizar un diagnóstico, brevemente describir el método utilizado para obtener acceso al equipo o sistemas afectados y qué vulnerabilidades fueron aprovechadas (clave fácil, deficiencia en los controles, etc.).

_____

_____

_____

Describa las medidas que fueron tomadas para atender el incidente:

Ninguna en especial

Reinstalación del sistema

Aplicación de parches

- Recuperación de copias de seguridad (Backups)
- Cambio de equipo
- Otra _____

Si existía algún plan escrito para manejar el incidente, describa de forma breve los pasos que siguió o anexe el documento.

Si en su opinión existen otros aspectos que se consideren importantes en el incidente, por favor descríbalos

_____

_____

2. INFORMACIÓN GENERAL

Área: _____

Nombre de la dependencia: _____

Responsable del sistema afectado (Persona con quién el equipo de seguridad & auditoría informática puede comunicarse y que conoce los detalles del incidente)

Nombres y Apellidos: _____

Cargo: _____

E-mail:_____ Teléfono: _____

Extensión: _____ Celular: _____ Fax: _____

Si sabe de otro equipo o sistema que haya sufrido el mismo problema o uno similar, diga cuál(es)

_____

_____

_____

3. INFORMACIÓN SOBRE EL EQUIPO AFECTADO

(Información sobre hardware, software y red. Si hay más sistemas, llene otro formato)

Dirección IP: _____Nombre del equipo: _____

Marca y modelo: _____

Capacidad de la RAM: _____ Capacidad del disco duro: _____

Modelo del procesador: _____

Sistema operativo (nombre y versión): _____

Función del equipo: _____

_____

_____

Tipo de información procesada por el equipo: _____

_____

Acto realizado por el Fiscal_____

Con la intervención de los Investigadores: _____y

Los Peritos Informáticos Forenses:_____

_____

En presencia del testigo:_____

Con CI _ RUN □ PASAPORTE N°_____

Observaciones:

_____

_____

_____

Con lo que termino el acto a horas……del día……de lmes……año.....……

Firmando al pie los intervinientes:

Fiscal:……

Investigador Asignado al caso:……..

Investigador Especial:……..

Perito Informático Forense (1):……

Perito Informático Forense (2):……

Propietario:……

Ocupante:……

Testigo:……

Otros:……

Figura 5: Formulario Solicitud Forense
Fuente: Elaboración propia

3.1.1.1. ASEGURAR LA ESCENA

Para asegurar que tanto los procesos como las herramientas a utilizar sean las más idóneas se debe contar con un personal competente a quien se le pueda asignar la conducción del proceso forense, para ello el equipo de seguridad debe estar capacitado y entender a fondo la metodología.

- Asegurar el acceso y control de los suministros de luz, ya que algunos equipos al ser apagados de manera incorrecta pueden dañarse (lo que haría irrecuperable la información).

- Si al momento de ingresar al lugar alguien se encuentra operando en el equipo o sistema involucrado en el posible ilícito, tomar nota de la situación y fotografiarlo cuando aún está sentado en posición de operador.

- Pedir a la persona que se encuentra en el equipo que suspenda de manera inmediata lo que está haciendo

- Una vez que se encuentra garantizado el cierre del área, proceder a tomar fotografías del estado y posición de los equipos, como así mismo de sus puertos (conectores de cables, lectores de CDs, lectores de disquets), es decir registrar en medio fotográfico o video la escena del hecho, detallando los elementos informáticos allí involucrados.

3.1.1.2. IDENTIFICAR LAS EVIDENCIAS

El siguiente paso y muy importante es la identificación de la evidencia presentada que es nuestra escena del crimen, la misma que estará sujeta a todos los procesos necesarios para la presentación de resultados finales. La evidencia se clasificara según:

3.1.1.3. PRIORIDADES DEL ADMINISTRADOR

Las evidencias se pueden clasificar según la prioridad del administrador, las mismas están basadas en la criticidad de los daños producidos por el incidente, una forma de clasificar los daños producidos es saber que tan críticos son y se lo encuentra aplicando la siguiente formula:

CRITICIDAD DE LOS DAÑOS	=	Extensión de daños producidos	+	Criticidad de los recursos afectados

✓ La extensión de los daños producidos es:

- Graves.- Que el incidente produjo daños muy severos sobre los servicios o información.
- Moderados.- Que el incidente causo molestias y pérdida de información.
- Leves.- Que el incidente producido no tiene mayor importancia, no se produjo ningún tipo de perdida pero si un corte o molestia en los servicios.

✓ La criticidad de los recursos afectados es:

- Alta.- Los recursos afectados son muy importantes dentro de la universidad y como tal comprometen el normal funcionamiento y prestación de servicios.

- Media.- Los recursos afectados causan molestias a un área de la universidad.

- Baja.- Los recursos afectados causan ciertas molestias pero se puede seguir con el normal funcionamiento de los equipos.

Un claro ejemplo de cómo obtener la criticidad de los daños producidos es utilizando las siguientes tablas:

Efectos del incidente y Recursos afectados						
Incidente	**Daños Producidos**			**Criticidad de los recursos Afectados**		
	Graves	Moderados	Leves	Alta	Media	Baja
Acceso no autorizado						
✓ Servidor Web	X			X		
✓ Servidor de archivos		X			X	
✓ Servidor de aplicaciones	X			X		
Infección de virus						
✓ Servidor			X		X	
✓ Estación de trabajo	X					X
✓ Etc.						

Estado de los recursos				
		Criticidad de los recursos afectados		
		Alta	Media	Baja
Daños producidos	Graves	Muy grave	Grave	Moderado
	Moderados	Grave	Moderado	Leve
	Leves	Moderado	Leve	Leve

Prioridad del administrador	
Estado	Prioridad
MUY GRAVE	10
GRAVE	7
MODERADO	4
LEVE	1

Tabla 2: Prioridad del Administrador

3.1.1.4. TIPO DE DISPOSITIVO

A las evidencias también se las puede clasificar según el tipo de dispositivo donde se las encuentre como:

- Sistemas informáticos
- Redes
- Redes Inalámbricas
- Dispositivos móviles
- Sistemas embebidos [6]
- Otros dispositivos

3.1.1.5. MODO DE ALMACENAMIENTO

A las evidencias también se las clasifica según el medio de almacenamiento. Como pueden ser:

- ✓ Volátiles.- Aquellas que se perderán al apagar el equipo como la hora del sistema y desfase de horario, contenido de la memoria, procesos en ejecución, programas en ejecución, usuarios conectados, configuración de red, conexiones activas, puertos abiertos, etc.

[6] ***Sistemas Embebidos*** La denominación de Sistemas embebidos (embedded) refleja que son una parte integral (interna) del sistema, y en general son dispositivos utilizados para controlar o asistir la operación de diversos equipamientos.

✓ No volátiles.- medios físicos de almacenamiento como memorias flash, CD, discos duros.



- Identificar los dispositivos informáticos que almacenen grandes volúmenes de información digital (computadora de escritorio, computadora portátil y discos duros portátiles

- Identificar memorias USBs, DVDs, CDs, disquets relevantes a la investigación

- Identificar si existen periféricos conectados a los equipos informáticos, realizar fotografías de las mismas.

- Identificar el posible delito que se hubiese cometido en la escena del hecho, determinar los presuntos actores involucrados, máquinas y/o usuarios y la posible participación que tuvo cada uno.

- Realizar entrevistas al personal de la organización que tenga algún tipo de relación con el entorno informático

- Identificar además las evidencias necesarias, electrónicas o no de la existencia de los vínculos entre el sujeto y el equipo, para lo cual se recomienda buscar, además de los bienes en sí mismos, los siguientes comprobantes de posible existencia:

  ✓ Comprobantes de pago y/o facturas de servicio de Internet, conexión satelital (teléfono y/o internet), facturas de luz, servicio de teléfono, servicio de telefonía celular, servicio de agua, tarjetas de crédito.
  ✓ Anotaciones de claves de usuario o de correos que pudieran encontrarse en soportes distintos a los electrónicos (papeles)

- ✓ Comprobantes de operaciones realizadas con tarjetas de crédito o débito.
- ✓ Comprobantes emitidos por cajeros automáticos.
- ✓ Listados de estados de cuentas bancarias.
- ✓ Plásticos o tarjetas de crédito o débito.
- ✓ Plásticos de tarjetas de hoteles u otras con banda magnética.
- ✓ Facturas de pago de cualquier comercio o institución que puedan relacionarse con la persona o con los números de tarjetas que utiliza o, en su caso con las cuentas bancarias, telefónicas o de internet que se investigan.

Entonces el primer proceso del análisis forense comprende la identificación, y búsqueda de evidencias. Se debe identificar qué cosas pueden ser evidencias, dónde y cómo está almacenada, qué sistema operativo se está utilizando. A partir de este paso, el equipo de seguridad puede identificar los procesos para la recuperación de evidencias adecuadas, así como las herramientas a utilizar.

3.2. FASE DE RECOPILACION

Si mediante los hallazgos del proceso de identificación de incidencias se comprueba que el sistema está comprometido, se requiere establecer la prioridad entre las alternativas de: levantar la operación del sistema o realizar una investigación forense detallada.

1) Generalmente la primera reacción suele ser restablecer el sistema a su estado normal, pero se debe considerar que esta actitud podría resultar en que se pierdan casi todas las evidencias que aún se encuentren en la "escena del delito" e incluso puede resultar en el impedimento de llevar a cabo las acciones legales pertinentes.

2) En el caso de que se elija la segunda alternativa y el profesional se encuentra capacitado para realizarlo, se debe iniciar con el proceso de

recopilar las evidencias que permitan determinar los métodos de entrada, actividades de los intrusos, identidad y origen, duración del evento o incidente, siempre precautelando evitar alterar las evidencias durante el proceso de recolección.

Hay que asegurarse de llevar un registro de cada uno de los pasos realizados y características o información de los hallazgos encontrados, es imprescindible tratar de obtener la mayor cantidad de información posible, así como también, es recomendable que durante el desarrollo de este proceso, lo asista u acompañe una persona, preferentemente imparcial, la misma que actuaría como testigo de dichas acciones y procedimientos realizados.

Recomendaciones que se deben tomar en cuenta para realizar la recopilación:

- ✓ Utilizar pulseras antiestáticas para evitar daños en los componentes electrónicos y guantes de látex para no alterar, encubrir o hacer desaparecer las huellas dactilares existentes en el equipo

- ✓ Tener los elementos necesarios: bolsas antiestáticas, sobres antihumedad, cajas de cartón (preferiblemente utilizar el material de embalaje que fue dispuesto por el fabricante de los dispositivos electrónicos que serán secuestrados)

- ✓ Proceder con el acordonamiento del lugar y asegurar el área donde ocurrió el incidente, con el fin de custodiar la escena del hecho y así fortalecer la cadena de custodia (ver Anexo C) y recopilación de la evidencia

- ✓ Según el RFC 3227[7] la evidencia debe ser recolectada de lo más a lo menos volátil. A continuación se presenta una posible clasificación según el orden de volatilidad:

- **Evidencia altamente volátil**

CPU (Registros, Caché), Memoria de Video. Usualmente la informacion en estos dispositivos es de mínima utilidad, pero debe ser capturada como parte de la imagen de la memoria del sistema.

- **Evidencia medianamente volátil**

La memoria RAM, incluye información sobre los procesos en ejecución, el hecho de capturarla hace que cambie. Requiere conocimiento especializado para poder reconstruirla, pero no se requiere mucho conocimiento para hacer una búsqueda de palabras clave. Tablas del Kernel (Procesos en ejecución), permiten analizar los procesos que pueden ser evidencia de actividades no autorizadas.

- **Evidencia poco volátil**

Medios Fijos (Discos Duros), Incluye área de swap, colas, directorios temporales, directorios de registros. La información recolectada en el área de swap y las colas permite analizar los procesos y la información de los mismos en un punto del tiempo en particular. Los directorios permiten reconstruir eventos.
Medio Removible (disquets, memorias USBs, CDs, DVDs), usualmente son dispositivos para almacenamiento de contenidos históricos del sistema. Si existen previamente a un incidente pueden ser usadas para acotar el periodo de tiempo

[7] RFC 3227 (Request For Comment) Petición de comentarios Documento que describe el orden de volatilidad de la evidencia digital

en el cual sucedió. Medio Impreso (papel), difíciles de analizar cuando hay muchos, ya que no se pueden realizar búsquedas automáticas sobre ellos.

Las evidencias que se recolecten de la escena del hecho, se transportan hasta los ambientes predefinidos, los laboratorios del Instituto de Investigación Forense, ambientes de la Fiscalía, o de ser necesario se transportan siempre apuntando la lista, en el cuaderno de investigaciones, bajo constancia en acta, con la firma de todos los participantes y un testigo de actuación[8]

3.3. FASE DE PRESERVACIÓN

Aunque el primer motivo de la recopilación de evidencias sea la resolución del incidente, puede ser que posteriormente se necesite iniciar un proceso legal contra los atacantes y en tal caso se deberá documentar de forma clara cómo ha sido preservada la evidencia tras la recopilación.

En esta fase, es imprescindible definir los métodos adecuados para el almacenamiento y etiquetado de las evidencias.

A considerar:

- ✓ Evitar tocar el material informático sin uso de guantes de látex, ya que dependiendo el objeto de la investigación, el teclado, monitores, mouse, disquets, CDs, DVDs, pueden ser utilizados para análisis de huellas dactilares.

[8] **NUEVO CODIGO DE PROCEDIMIENTO PENAL – BOLIVIA: Artículo 121º.- (Testigos De Actuación).** Podrá ser testigo de actuación cualquier persona con excepción de los menores de catorce años, los enfermos mentales y los que se encuentren bajo el efecto de bebidas alcohólicas o estupefacientes

- ✓ No permitir que personal no idóneo manipule la evidencia digital, pues podría dañar, modificar y/o destruir información importante que podría servir para el esclarecimiento de un delito informático.

- ✓ Realizar un informe y hacer conocer si la evidencia digital ha sido previamente manipulada por personal no idóneo, ya que al realizar el análisis de datos y detectar que la información original ha sido alterada, la evidencia pierde su valor probatorio.

- ✓ En muchos casos no se puede realizar copias de la evidencia original por impedimentos técnicos u otras razones de tiempo y lugar. En estos casos tener mayor cuidado de preservar la evidencia digital, pues de ocurrirse un daño probablemente no se podrá obtener nuevamente la evidencia tal como se encontró en primera instancia.

- ✓ Usar bolsas especiales antiestáticas para almacenar disquets, CDs, DVDs y otros dispositivos de almacenamiento informáticos que sean electromagnéticos (si no se cuenta, pueden utilizarse bolsas de papel madera). Evitar el uso de bolsas plásticas, ya que pueden causar una descarga de electricidad estática que puede destruir los datos.

- ✓ Mantener la cadena de custodia del material informático transportado y llenar el acta para cadena de custodia en el caso de delitos informáticos (ver Figura 5, pág.59),

- ✓ Preservar y resguardar el material informático en ambientes donde no deberán exponerse a campos electromagnéticos, además donde el acceso a dichos ambientes sea estrictamente controlado. Los elementos informáticos son frágiles y deben manipularse con precaución, por personas idóneas en la manipulación de evidencia digital.

- ✓ El punto clave en la preservación de la evidencia digital es que se recolecte sin alterarla y evitar su manipulación futura, si se contará con entidades de

certificación quienes expiden certificados de firma digital que pueden ser útiles para estos procesos, sería un gran respaldo, lamentablemente en la actualidad en nuestro país no contamos con éste tipo de entidades.

Una vez que se cuenta con todas las evidencias del incidente es necesario conservarlas intactas ya que son las "huellas del crimen", se deben asegurar estas evidencias a toda costa. Para ello se sigue el siguiente proceso:

3.3.1. COPIAS DE LA EVIDENCIA

Como primer paso se debe realizar dos copias de las evidencias obtenidas, generar también una suma de comprobación de la integridad de cada copia mediante el empleo de funciones hash tales como MD5 o SHA1.

El valor hash es una cadena de caracteres y números, obtenida a través de un algoritmo estándar (HASH o función resumen) aprobado internacionalmente los más utilizados son el MD5 y el SHA-1, a partir de un conjunto de datos, los valores hash generados por dicho algoritmo son únicos.

El valor hash obtenido también debe registrarse en el formulario de adquisición de evidencia digital, para demostrar la integridad y autenticidad de la evidencia digital original, el cual ayudará a probar que no se ha alterado la evidencia luego de que la computadora llego a su posesión, para negar alegatos de que se ha cambiado la información original.

Incluir estas firmas en la etiqueta de cada copia de la evidencia sobre el propio medio de almacenamiento como CD o DVD etiquetado la fecha y hora de creación de la copia, nombre cada copia, por ejemplo "COPIA A", "COPIA B" para distinguirlas claramente del original.

Si además se extrae los discos duros del sistema para utilizarlos como evidencia, se debe seguir el mismo procedimiento, colocando sobre ellos la etiqueta "EVIDENCIA ORIGINAL", incluir además las correspondientes sumas

hash, fecha y hora de la extracción del equipo, datos de la persona que realizó la operación, fecha, hora y lugar donde se almacenó, por ejemplo en una caja fuerte.

Tener en cuenta que existen factores externos como cambios bruscos de temperatura o campos electromagnéticos que pueden alterar la evidencia. Toda precaución es poca, incluso si decide enviar esos discos a que sean analizados por empresas especializadas.

3.3.2. CADENA DE CUSTODIA

Otro aspecto muy importante es la cadena de custodia, donde se establecen las responsabilidades y controles de cada una de las personas que manipulen la evidencia. Se debe preparar un documento en el que se registren los datos personales de todos los implicados en el proceso de manipulación de las copias, desde que se tomaron hasta su almacenamiento.

El documento debe contener la siguiente información:

- ✓ Dónde, cuándo y quién examinó la evidencia, incluyendo su nombre, su cargo, un número identificativo, fechas y horas, etc.
- ✓ Quién estuvo custodiando la evidencia, durante cuánto tiempo y dónde se almacenó.
- ✓ Cuando se cambie la custodia de la evidencia también se deberá documentar cuándo y cómo se produjo la transferencia y quién la transportó.

Todas estas medidas harán que el acceso a la evidencia sea muy restrictivo quedando claramente documentado, posibilitando detectar y pedir responsabilidades ante manipulaciones incorrectas, intentos de acceso no autorizados o que algún otro dispositivo electromagnético se use dentro de un determinado radio.

La cadena de custodia es esencial, pues en caso de adulteración de la prueba, nos permitiría investigar las causas, y posibles responsables.

La cadena de custodia deberá contener información sobre el dispositivo incautado, número de serie, fabricante, y una descripción detallada acerca de quienes han tenido en su poder la evidencia, sus razones, procedimientos, y los detalles sobre la fecha y la hora exacta de todos estos sucesos (ver figura 5).

Identificación de Evidencias y Cadena de Custodia

Fecha: _____ Delitos: _____

Normas Legales Infringidas: _____

N° Caso: _____ Fiscal Adjunto: _____

Lugar de Recolección
(Local y Dirección): _____

Fecha de Recolección: _____ Hora de Recolección: _____

Fuente de la Evidencia: _____

Nombre e identificación de
persona fuente de evidencia: _____

Nombre posición e institución
de quien recopilo la evidencia: _____

Datos de Evidencia:

Número de la evidencia en el sitio del suceso y/o en el caso: _____

Tipo: _____

Descripción: _____

Características físicas: _____ Números seriales: _____

N°	Entregada por: (Nombre e Institución)	Firma	Recibida por: (Nombre e Institución)	Firma	Fecha y Hora	Motivo (Almacenamiento, Inspección, Pericia, Traslado, Disposición Final)
1						
2						
3						
4						
5						

Figura 6: Acta para la identificación y cadena de custodia
Fuente: Elaboración propia

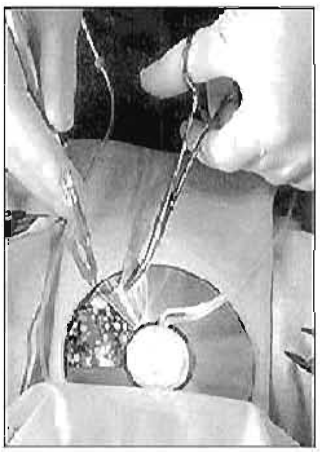
3.4. FASE DE ANÁLISIS

Antes de iniciar esta fase se deben prepararlas herramientas, técnicas, autorizaciones de monitoreo y soporte administrativo para iniciar el análisis forense sobre las evidencias obtenidas o presentadas por el administrador de los servidores.

Una vez que se dispone de las evidencias digitales recopiladas y almacenadas de forma adecuada, iniciamos la fase más laboriosa, el Análisis Forense propiamente dicho, cuyo objetivo es reconstruir con todos los datos disponibles la línea temporal del ataque, determinando la cadena de acontecimientos que tuvieron lugar desde el inicio del ataque, hasta el momento de su descubrimiento.
Este análisis se dará por concluido cuando se descubra cómo se produjo el ataque, quién o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron, etc. En el proceso de análisis se emplean las herramientas propias del sistema operativo (anfitrión) y las que se prepararon en la fase de extracción y preparación.

3.4.1. PREPARACIÓN PARA EL ANÁLISIS

Antes de comenzar el análisis de las evidencias se deberá:



1) Acondicionar un entorno de trabajo adecuado al estudio que se desea realizar.

2) Trabajar con las imágenes que se recopiló como evidencias, o mejor aún con una copia de éstas, tener en cuenta que es necesario montar las imágenes tal cual estaban en el sistema comprometido.

3) Si dispone de recursos suficientes preparar dos estaciones de trabajo, una de ellas contendrá al menos dos discos duros.

4) Instar un sistema operativo que actuará de anfitrión y que servirá para realizar el estudio de las evidencias. En este mismo ordenador y sobre un segundo disco duro, instalar las imágenes manteniendo la estructura de particiones y del sistema de archivos tal y como estaban en el equipo atacado.

5) En otro equipo instar un sistema operativo configurado exactamente igual que el equipo atacado, además mantener nuevamente la misma estructura de particiones y ficheros en sus discos duros. La idea es utilizar este segundo ordenador como "conejillo de Indias" y realizar sobre él pruebas y verificaciones conforme se vayan surgiendo hipótesis sobre el ataque.

Si no se dispone de estos recursos, se puede utilizar software como VMware, que permitirá crear una plataforma de trabajo con varias máquinas virtuales [3]. También se puede utilizar una versión LIVE de sistemas operativos como Linux, que permitirá interactuar con las imágenes montadas pero sin modificarlas. Si se está muy seguro de las posibilidades y de lo que va a hacer, se puede conectar los discos duros originales del sistema atacado a una estación de trabajo independiente para intentar hacer un análisis en caliente del sistema, se deberá tomar la precaución de montar los dispositivos en modo sólo lectura, esto

se puede hacer con sistemas anfitriones UNIX/Linux, pero no con entornos Windows.

3.4.1.1. PASOS PARA REALIZAR UN ANÁLISIS DE DATOS FORENSE:

Es necesario seguir una serie de pasos para la obtención de la evidencia digital. A continuación se propone una guía que organiza y reúne una serie de actividades es necesario definir un conjunto de elementos requeridos que constituyen la información inicial. Estos elementos son:

- ✓ Imágenes binarias de los dispositivos de almacenamiento digital comprometidos en el caso con sus respectivos compendios criptográficos.
- ✓ Descripción del caso ilustrado en el marco circunstancial.

- ✓ Metadatos de cada una de las imágenes, es decir, todo tipo de información necesaria para determinar las características de la imagen en particular.

Descripción de los pasos:

1. *Creación del archivo de hallazgos*

Consiste en la creación y el aseguramiento de un documento, ya sea físico o electrónico, que permita llevar un historial de todas las actividades que se llevan a cabo durante el proceso y de los hallazgos encontrados de modo que se tenga un resumen que permita hacer la reconstrucción del caso tiempo después de que este hay asido analizado (ver figura 6).

2. *Imagen de datos*

Consiste en la recepción de las imágenes de datos que conciernen al caso en investigación.

3. *Verificación de integridad de la imagen*

Par cada imagen suministrada debe calcular su compendio criptográfico (MD5), comparándolo luego con el de la fuente original si la comparación arroja un resultado negativo se debe rechazar la imagen proveída en el paso.

4. *Creación de una imagen de la copia suministrada*

En un análisis de datos nunca se debe trabajar sobre la imagen original suministrada sino sobre una copia.

5. *Aseguramiento de la imagen suministrada*

Se debe garantizar que la imagen suministrada no sufra ningún tipo de alteración, con el fin de conservación de la cadena de custodia y del mantenimiento de la validez jurídica de la evidencia.

6. *Revisión antivirus y verificación de la integridad de la copia de la imagen*

Una vez que se haya obtenido la copia de la imagen, es necesario asegurarse que no tenga ningún tipo de virus conocido.

Luego se debe verificar la integridad de la copia, de la misma forma como se hizo con la original (paso 2). De hecho, esta actividad es transversal en la técnica es decir, debe realizarse periódicamente durante el proceso de análisis de datos, de modo que se garantice la integridad de la evidencia desde el comienzo hasta su culminación de la investigación.

7. *Identificación de las particiones actuales y anteriores (las que sea posible recuperar)*

La identificación de las particiones en un dispositivo es de vital importancia, ya que reconocerla implica la identificación de sus archivos, mediante el cual se pueden conocer características especiales de la organización de la información y se puede definir la estrategia de recuperación de archivos adecuada.

8. *Detección de información en los espacios entre las particiones*

Cuando se detectan datos en estas zonas de la imagen, se debe proceder a hacer un análisis para determinar si representan algún tipo de información relevante para la investigación. En caso de estar protegidos estos archivos serán tenidos en cuenta en la etapa de identificación de archivos protegidos.

9. *Identificación del sistema de archivos*

Para cada una de las particiones identificadas en el paso 6, debe identificarse su sistema de archivos, con el fin de escoger la forma de realizar actividades posteriores del análisis de datos.

10. *Recuperación de los archivos borrados*

Durante esta actividad se debe tratar de recuperar los archivos borrados del sistema de archivos, lo que es conveniente, dado el frecuente borrado de archivos para destruir la evidencia

Dependiendo de las características técnicas y del estado del sistema de archivos, puede no ser posible la recuperación de la totalidad de los archivos eliminados; por ejemplo, si estos han sido sobre escritos, o si se han utilizado herramientas de borrado seguro para eliminarlos.

Los archivos recuperados exitosamente formarán parte de los archivos potencialmente analizables, exceptuando los archivos identificados como protegidos que serán tenidos en cuenta durante la fase de identificación de archivos protegidos.

11. *Recuperación de información escondida*

En esta etapa se debe examinar exhaustivamente los campos reservados en el sistema de archivos y los espacios etiquetados como dañados por el sistema de archivos.

Al igual que en la etapa 9, los archivos protegidos también se tendrán en cuenta durante la etapa de análisis de este tipo de archivos.

12. *Identificación de archivos existentes*

Seguidamente se clasifican los archivos restantes entre protegidos y no protegidos, donde estos últimos harán parte de los archivos potencialmente analizables, mientras los primeros harán parte en la etapa de análisis de archivos protegidos.

13. *Identificación de archivos protegidos*

Esta es la tapa e consolidación de archivos protegidos identificados en las etapas anteriores. Durante esta fase se pretende descifrar o romper tal protección en estos archivos, con el fin de adicionarlos al conjunto de archivos potencialmente analizables. Los archivos cuya protección no pudo ser vulnerada formaran parte del conjunto de archivos sospechosos.

14. *Consolidación de archivos potencialmente analizables*

Durante esta etapa se reúnen todos los archivos encontrados durante las fases de recuperación de archivos borrados, recuperación de información escondida, identificación de archivos existentes e identificación de archivos protegidos.

15. *Determinación del sistema operativo y las aplicaciones*

Al terminar el sistema operativo y las aplicaciones instaladas, se está en la capacidad de obtener la lista de compendios criptográficos de los archivos típicos del sistema operativo y de las aplicaciones, para verificar posteriormente la integridad de estos archivos de encontrarse en la imagen sometida a análisis.

16. *Filtrado basado en archivos buenos conocidos*

Con la lista de compendios criptográficos obtenida en el paso anterior, se procede a verificar la integridad de los archivos en la imagen que aparecen en tal lista. Si dicha comprobación es exitosa, este se considera "bueno" y por lo tanto, es descartado el proceso de análisis.

17. *Consolidación de archivos sospechosos*

Como resultado del filtrado de "buenos" conocidos se obtiene un conjunto de archivos susceptibles a análisis, este conjunto se llamará archivos sospechosos.

18. *Primera clasificación*

Divide los archivos sospechosos en:

- archivos "buenos" modificados: son identificados en la fase de filtrado como archivos buenos cuya versión original (descrita por la lista obtenida en el paso 14)
- archivos "malos": se obtienen a partir de la comparación de los archivos sospechosos contra los compendios criptográficos de archivos "malos" relacionados con el sistema operativo particular.

  Estos archivos representan algún tipo de riesgo para el sistema en el que se encuentran o ejecutan,, por ejemplo: troyanos, virus entre otros.
- Archivos con extensión modificada: aquellos cuya extensión no es consistente con su contenido.

Los archivos que cumplen alguna de las anteriores características se convierten en prioritarios para el análisis. Los que no cumplen se someten a la siguiente etapa de clasificación.

19. *Segunda clasificación*

Esta clasificación toma archivos que no han sido considerados de máxima prioridad, los examina y los evalúa respecto a dos criterios: relación de los archivos con los usuarios involucrados en la investigación y contenido relevante para el caso, derivado del marco circunstancial.

20. *Analizar los archivos*

Este proceso se basa en la discriminación de los archivos prioritarios con respecto a su relevancia con el caso y el criterio del investigador.

Es importante resaltar que los procesos de la segunda clasificación y análisis, pueden ser iterativos con el fin d obtener de la segunda clasificación y

análisis, pueden ser iterativos con el fin de obtener más cantidad de evidencia pertinente. En cada iteración cada archivo d alta prioridad puede ser descartado o catalogado como archivo comprometido en el caso, y los archivos con poca prioridad son sometidos a una nueva iteración.

21. *Archivos comprometidos con el caso*

Es el conjunto d archivos que forman parte d la evidencia del caso.

22. *Obtención de línea de tiempo*

Se procede a realizar la reconstrucción de los hechos a partir de los atributos de tiempo de los archivos, lo que permiten correlacionarlos enriqueciendo la evidencia.

Es importante resaltar que en algunas ocasiones y dependiendo del sistema de archivos del volumen analizados, puede ser imposible realizar uh análisis temporal situación que, como todos los hallazgos, debe ser consignado en el informe.

23. *Generación del informe*

Se elabora el informe de hallazgos, que contiene una descripción detallada de los hallazgos relevantes al caso y la forma como fueron encontrados, apoyándose en la documentación continua de la aplicación técnica

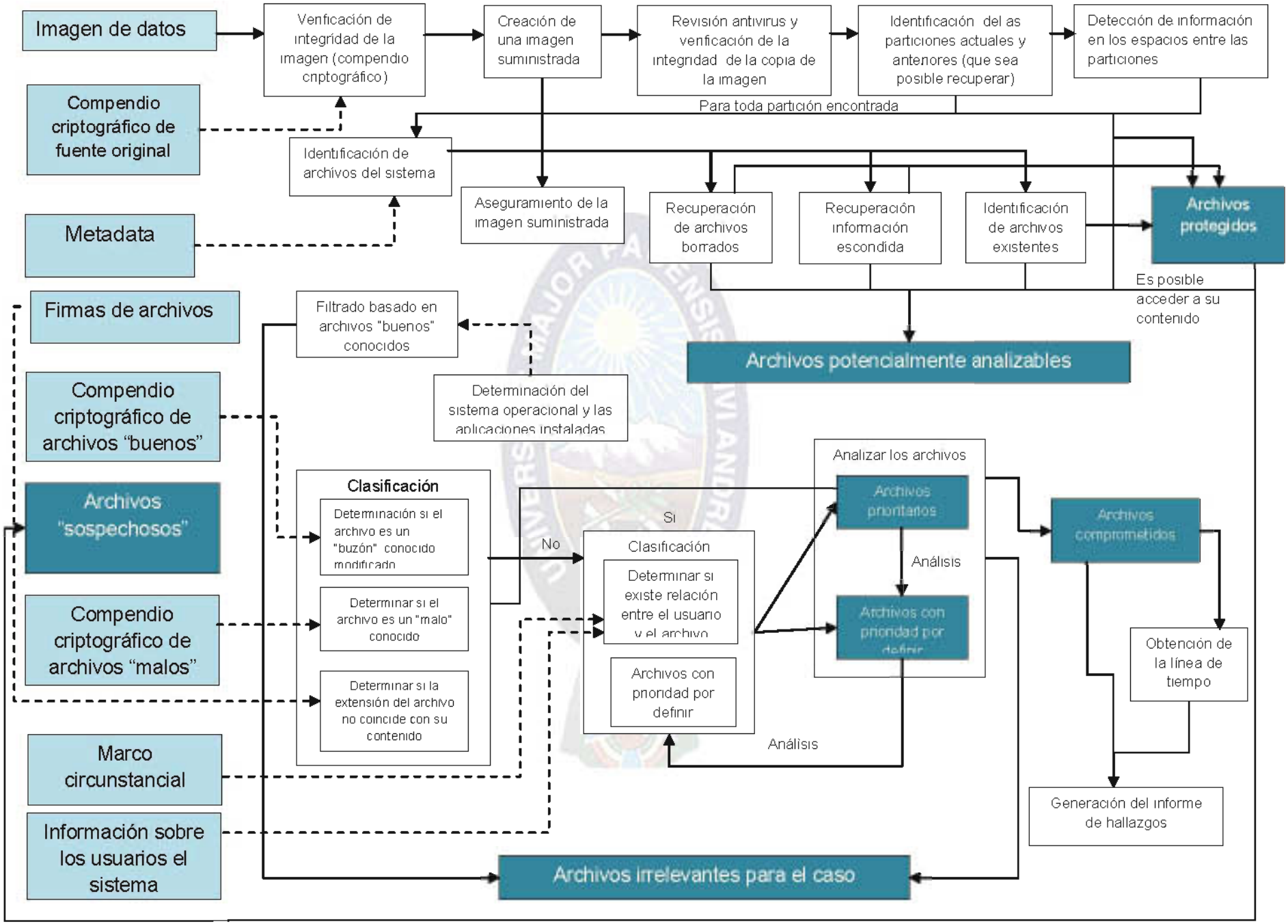


Figura 7: Fase de Análisis- pasos para realizar un análisis de la evidencia digital

3.5. FASE DE DOCUMENTACIÓN Y PRESENTACIÓN DE LAS PRUEBAS

Es muy importante comenzar a tomar notas sobre todas las actividades que se lleven a cabo. Cada paso dado debe ser documentado y fechado desde que se descubre el incidente hasta que finaliza el proceso de análisis forense, esto permitirá ser más eficiente y efectivo al tiempo que se reducirá las posibilidades de error a la hora de gestionar el incidente.

3.5.1. UTILIZACIÓN DE FORMULARIOS DE REGISTRO DEL INCIDENTE

Es importante que durante el proceso de análisis se mantenga informados a los administradores de los equipos y que tras la resolución del incidente se presenten los informes Técnico y Ejecutivo. El empleo de formularios puede ayudarle bastante en este propósito. Éstos deberán ser rellenados por los departamentos afectados o por el administrador de los equipos. Alguno de los formularios que debería preparar serán:

- Documento de custodia de la evidencia
- Formulario de identificación del equipos y componentes
- Formulario de incidencias tipificadas
- Formulario de publicación del incidente
- Formulario de recogida de evidencias
- Formulario de discos duros.

3.6. PROCEDIMIENTO PARA QUE LA EVIDENCIA DIGITAL SEA ADMITIDA EN BOLIVIA

De aplicarse al inicio o en cualquier etapa procedimental pruebas nulas, de dudosa obtención o que afecten garantías constitucionales como la privacidad, el que nadie puede ser obligado a declarar en su propia contra o cualquier otra, de hecho la

investigación y el mismo proceso tendrán en su interior el mismo defecto que arrastran desde sus inicios, por lo cual serán nulas o inadmisibles en un juicio, según el Nuevo Código de Procedimiento Penal (NCPP) vigente en Bolivia.

NCPP - BOLIVIA: Artículo 13º.- (Legalidad de la Prueba)

I. *Los elementos de prueba sólo tendrán valor si han sido obtenidos por medios lícitos e incorporados al proceso conforme a las disposiciones de la Constitución Política del Estado y de este Código.*

II. *No tendrá valor la prueba obtenida mediante torturas, malos tratos, coacciones, amenazas, engaños o violación de los derechos fundamentales de las personas, ni la obtenida en virtud de información originada en un procedimiento o medio ilícito.*

NCPP - BOLIVIA: Artículo 71º.- (Ilegalidad de la Prueba).

Los fiscales no podrán utilizar las pruebas obtenidas en contra del imputado en violación a la Constitución Política del Estado, Convenciones y Tratados internacionales vigentes y las leyes.

Con la finalidad de que no existan nulidades procedimentales, es necesario que se cuente con una orden judicial o requerimiento de un fiscal, para poder realizar la identificación, adquisición y preservación de la evidencia digital puesto que al no compartir las características de los demás bienes, no se puede tomar una orden de cateo genérico como suficiente, púes con éste no podremos realizar ningún tipo de inspección a los sistemas electrónicos o en otro caso asegurarlos.

La apertura de un equipo informático o bien su aseguramiento implica la posibilidad de violentar garantías constitucionales, lo que, en definitiva debe ser siempre ordenado y controlado por un juez competente.

El Ministerio Público [8] debe solicitar de manera expresa el aseguramiento de los medios y equipos electrónicos que pudieran contener información. Con las respectivas previsiones, la evidencia contenida en los equipos o en los medios asegurados puede ser incorporada correctamente al expediente (averiguación previa o proceso judicial) sin objeciones sobre la legalidad de su obtención, pues se estuviese respetando de manera plena las garantías constitucionales involucradas en el proceso.

El Ministerio Público debe incluir en su solicitud expresa la recolección de información y/o el vaciado de datos (copia bit a bit), ya que se puede dar el caso de que el aseguramiento sea físicamente imposible, pues varios equipos no pueden ser movidos en relación directa con su tamaño o bien con el hecho de que de ser retirados podría perderse información de los registros que se están procesando al momento del operativo.

El profesional informático forense en una investigación de delitos informáticos llega a ser un perito de ésta disciplina, quien en algunos casos trabajará en una misma escena del hecho con otros peritos, por lo cual es indispensable tomar previsión de solicitar al juez o al fiscal según sea el caso, la facultad de fotografiar y filmar, realizar extracciones de datos en el momento (en la escena del hecho).

Para que los otros peritos que acompañan al Ministerio Público en el acto puedan tomar los recaudos necesarios y permitir dichas actividades, previo el visto bueno de la autoridad competente que da curso a la solicitud.
del equipo para que estas puedan, luego ser objeto de las pruebas periciales que se requieran.

---

[8] **Ministerio Público** - Órgano constitucional que tiene por finalidad promover la acción de la justicia, defender la legalidad, los intereses del Estado y la Sociedad, representándolos conforme a lo establecido en la Constitución y en las Leyes de la República. Es único e indivisible y ejerce sus funciones a través de los fiscales, quienes lo representan íntegramente **[Ley Orgánica Ministerio Público, Bolivia]**

Estas solicitudes incluyen, según el caso la posibilidad de apertura de claves (en caso que se tenga información cifrada) por procedimientos informáticos si estas existen y el equipo no puede ser retirado, o bien el retiro parcial de algunas partes

El delito informático de acuerdo al Art. 363 bis y 363 ter del Código Penal de Bolivia (ver Anexo B) debe producir daño o transferencia patrimonial. El perito informático dirá sobre los aspectos técnicos, mas no podrá concluir sobre el daño o beneficio económico, para tal efecto necesitará considerar la figura de un perito contable o perito financiero quien en base a los datos e información validada por el perito informático podrá decir sobre la cuantía del daño. Para definir la selección del perito, se debe tomar en cuenta en primer lugar el ordenamiento legal que se tiene en nuestro país:

NCPP - BOLIVIA: Artículo 204º.- (Pericia).

Se ordenará una pericia cuando para descubrir o valorar un elemento de prueba sean necesarios conocimientos especializados en alguna ciencia, arte o técnica

NCPP – BOLIVIA: Artículo 205º.- (Peritos).

I. *Serán designados peritos quienes, según reglamentación estatal, acrediten idoneidad en la materia.*

II. *Si la ciencia, técnica o arte no está reglamentada o si no es posible contar con un perito en el lugar del proceso, se designará a una persona de idoneidad manifiesta.*

III. *Las reglas de este Título regirán para los traductores e intérpretes. Más sobre los peritos y el ordenamiento legal vigente en nuestro país*

En un proceso penal, si la obtención de la evidencia digital afecta cualquier otro derecho constitucional o no es adecuada al cumplimiento de las garantías del debido proceso, dichas evidencias no pueden ser usadas en el juicio en contra del supuesto delincuente, lo que aumentaría notablemente la situación de impunidad que actualmente existe en materia de delitos informáticos o cometidos por medios informáticos, e incluso en delitos comunes donde la evidencia digital contenida en elementos electrónicos pudiere apoyar la investigación o condena de los criminales.

Bajo toda circunstancia se debe mantener la cadena de custodia, que es el mecanismo que garantiza la autenticidad de los elementos probatorios recolectados y analizados. Esto significa, que las pruebas correspondan al caso investigado sin que se dé lugar a confusión, adulteración, pérdida, ni sustracción alguna. Por lo tanto, todo funcionario que participe en el proceso de cadena de custodia debe velar por la seguridad, integridad y preservación de dichos elementos.

La cadena de custodia garantiza que el perito informático reciba del investigador especial y/o fiscal, los elementos de prueba en el mismo estado en que fueron percibidos en la escena del hecho, igualmente que sean devueltos al investigador en la misma situación, que al ser presentados ante el tribunal se pueda comprobar su autenticidad y no existan dudas sobre la misma. Conforme lo dispuesto en el Art. 295 inciso 12 del Código de Procedimiento Penal vigente en nuestro país "Custodiar, bajo inventario, los objetos secuestrados" es decir toda transferencia de custodia debe quedar consignada en el Acta para Cadena de Custodia en el Caso de Delitos Informáticos indicando: fecha, hora, nombre y firma de quién recibe y de quién entrega. La naturaleza de los medios de almacenamiento digital, corren el riesgo de cambiar su estado o sufrir daños de transporte y conservación, debiendo la Fiscalía proveer las medidas para garantizar su

permanencia en el tiempo, amparados en el Nuevo Código de Procedimiento Penal de Bolivia Art. 186.

NCPP - BOLIVIA: Artículo 186°.- (Procedimiento para el Secuestro)

I. *Regirá el procedimiento establecido para el registro. Los objetos secuestrados serán inventariados y puestos bajo segura custodia en los depósitos de la Fiscalía o en los lugares especialmente destinados para estos efectos, bajo responsabilidad y a disposición del fiscal.*

II. Los semovientes, vehículos y bienes de significativo valor serán entregados a sus propietarios o a quienes acrediten la posesión o tenencia legítima, en calidad de depositarios judiciales después de realizadas las diligencias de comprobación y descripción.

III. *Si los objetos secuestrados corren riesgo de alterarse, desaparecer, sean de difícil conservación o perecederos, se ordenarán reproducciones, copias o certificaciones sobre su estado y serán devueltos a sus propietarios.*

Se podrá pedir el anticipo de prueba, si no existiesen garantías de traslado, es decir que no exista la seguridad de que al momento de realizarse el traslado la evidencia digital no sufra modificación alguna. Por ejemplo el riesgo de traslado es mayor en evidencias con componentes mecánicos que pueden desincronizarce como en el caso de los Discos Duros.

NCPP - BOLIVIA: Artículo 307° (Anticipo de prueba)

I. Cuando sea necesario practicar un reconocimiento, registro, reconstrucción o pericia, que por su naturaleza o características se consideren como actos definitivos e irreproducibles, o cuando deba recibirse una declaración que, por algún obstáculo, se presuma que no podrá producirse durante el juicio, el fiscal o cualquiera de las partes podrán pedir al juez que realice estos actos.

II. El juez practicará el acto, si lo considera admisible, citando a todas las partes, las que tendrán derecho a participar con las facultades y obligaciones previstas en este Código.

III. Si el juez rechaza el pedido, se podrá acudir directamente al tribunal de apelación, quien deberá resolver dentro de las veinticuatro horas de recibida la solicitud, ordenando la realización del acto, si lo considera admisible, sin recurso ulterior. En casos de evidencia digital, es recomendable que cuando no exista la posibilidad de garantizar un ambiente de conservación adecuado, la Fiscalía apoyada en el Artículo 307 del Nuevo Código de Procedimiento Penal de Bolivia, pueda generar medidas que garanticen la permanencia inalterable de la evidencia digital, ya que la preservación de la evidencia digital es vital, pues ésta es frágil y puede ser fácilmente alterada o destruida. Muchas veces esta alteración puede ser irreversible.

3.6.1. GARANTÍAS A CUBRIR

- ***El valor probatorio:***

En la realidad de los procesos penales, esta situación depende de la propia valoración que pueda dar el juez interviniente a las evidencias digitales que se aporten a la causa, de manera que cuanto mayor sea la información que pueda obtenerse de los equipos electrónicos que se catean y aseguran, mayor podrá ser la relevancia para una sentencia absolutoria o condenatoria según el caso de que se trate. En realidad depende de un segundo factor que es la credibilidad que pueda tenerse en adquirir y conservar los equipos y la evidencia en ellos contenida, como así también en la inviolabilidad o no adulteración de esos contenidos a favor o en contra del sujeto a proceso.

- ***La inviolabilidad de los contenidos:***

De hecho este es en realidad el punto medular de la cuestión probatoria, ya que como se dijo, si la evidencia puede ser manipulada o es obtenida de forma ilegal, no sólo se corre el riesgo de que resulte inadmisible sino también de que con ella puedan caer partes importantes del proceso que podrían resultar en que un sujeto pudiera obtener su libertad aun cuando sea claramente responsable del hecho que se le imputa. Teniendo en cuenta que es la representación social quien debe probar la culpabilidad, pues se presume la inocencia del encausado mientras no se pruebe su culpabilidad (*NCPP Art. 6º.- Presunción de Inocencia)* y sin las pruebas necesarias, o bien con ellas pero inadmisibles, esto resulta imposible para la parte acusadora quien vera disolverse sus posibilidades de manera directa al grado de errores en la búsqueda y recolección de bienes electrónicos.

NCPP - BOLIVIA: Artículo 6º.- (Presunción de Inocencia).

1. *Todo imputado será considerado inocente y tratado como tal en todo momento, mientras no se declare su culpabilidad en sentencia ejecutoriada.*
2. *No se podrá obligar al imputado a declarar en contra de sí mismo y su silencio no será utilizado en su perjuicio.*
3. *La carga de la prueba corresponde a los acusadores y se prohíbe toda presunción de culpabilidad.*
4. *En el caso del rebelde, se publicarán únicamente los datos indispensables para su aprehensión.*

Los errores que se cometen son los que coadyuvan a la inadmisibilidad de las pruebas, siendo que a través de las cuales se podrían condenar o absolver a los indiciados, es imprescindible tratar de reducirlos al mínimo para que los elementos

que puedan ser usados como prueba y la información que ellos contienen adquieran relevancia a la hora en que el decidor deba pronunciarse a través de la sentencia.

- ***La Privacidad :***

En procesos donde se involucre información contenida en equipos electrónicos, una de las garantías a cubrir es la privacidad, dado que si el sujeto titular de la información y en su caso propietario o poseedor del medio de soporte la colocó en ese formato, es para que no pueda ser accedida simplemente y sin su autorización expresa.

De hecho esta debemos tener presente que siempre es una garantía relativa, pues puede caer ante la orden expresa de un juez, pero siempre que se respeten los principios que le dan sustento, es decir que por ejemplo para la apertura de un correo electrónico se respeten las garantías que atañen a la comunicación postal. En la Nueva Constitución Política del Estado (NCPE - Bolivia), el artículo más cercano al Habeas Data (Recurso para la protección de privacidad) se encuentra en:

NCPE - BOLIVIA: Artículo 130
(Acción de Protección de Privacidad)

I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.

II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa.

3.7. DEMOSTRACION

3.7.1. DEMOSTRACION DE LA HIPOTESIS

Un razonamiento es deductivo si y solo si las premisas son evidencia de la verdad de la conclusión [Rojo, 1996], para tal efecto nos basaremos en el razonamiento Deductivo Válido

3.3.1.1 Autenticidad

La autenticidad de la evidencia nos sugiere ilustrar a las partes en conflicto, que dicha evidencia ha sido generada y registrada en los lugares o sitios relacionados con el caso, particularmente en la escena del hecho o lugares establecidos en la diligencia de levantamiento de evidencia. Así mismo, la autenticidad, entendida como aquella característica que muestra la no alterabilidad de los medios originales, busca confirmar que los registros aportados corresponden a la realidad evidenciada. Éste concepto se puede apreciar claramente en todos los procedimientos:

En la fase de identificación de la evidencia digital a secuestrar con la toma de fotografías, filmaciones del estado y posición de los equipos en la escena del hecho, el levantamiento del mapa de elementos informáticos involucrados se garantiza la autenticidad de la evidencia digital.

En la fase para recopilar la evidencia digital se diferencian los componentes uno del otro por medio de etiquetas numeradas y firmadas, se realiza fotografías del número que se asigna a cada equipo. Con la extracción original de datos (copia bit a bit) de la cual al obtenerse el valor hash existe un medio más para probar la autenticidad de la evidencia, además de las características de las evidencias, números de serie, el

valor hash también se registra en el formulario de adquisición de evidencia digital, se realiza el precintado de los puertos y de componentes que puedan ser abiertos.

En la fase para preservar la evidencia digital la cadena de custodia es el mecanismo que garantiza la autenticidad de los elementos probatorios adquiridos y analizados.

Esto significa, que las pruebas correspondan al caso investigado sin que se dé lugar a confusión, adulteración, pérdida, ni sustracción alguna. Por lo tanto, todo funcionario que participe en el proceso de cadena de custodia vela por la seguridad, integridad y preservación de dichos elementos.

En la fase para analizar la evidencia digital, el concepto de autenticidad se logra al realizar el análisis con herramientas forenses (con licencia).

En medios no digitales, la autenticidad de las pruebas aportadas no será refutada, de acuerdo por lo dispuesto en el Art. 216 del Nuevo Código de Procedimiento Penal:

NCPP-BOLIVIA: Artículo 216°.- (Documentos).

I. Se admitirá toda prueba documental lícitamente obtenida.
II. El imputado no podrá ser obligado a reconocer documentos privados que obren en su contra, debiendo el juez o tribunal interrogarle si está dispuesto a declarar sobre su autenticidad, sin que su negativa le perjudique.

En este caso, las partes podrán acreditar la autenticidad por otros medios. En el procedimiento para que la evidencia digital sea permitida legalmente se dan a conocer los aspectos legales que se debe considerar: presencia de un fiscal, orden judicial o requerimiento de un fiscal antes de empezar la aplicación del método informático forense, se debe anotar todo lo que se realiza en el cuaderno de investigaciones, bajo constancia en el acta de allanamiento con la firma de todos los participantes y los testigos de actuación, para descartar que esa evidencia fue

adquirida de manera ilegal y además para respaldar que fue levantada de la escena del hecho y autenticar que la evidencia proviene del incidente en cuestión. Por todo lo expuesto anteriormente, el método informático forense garantiza la autenticidad de la evidencia digital, de tal afirmación obtenemos la siguiente premisa:

p = La evidencia digital es auténtica

3.3.1.2 Confiabilidad

La confiabilidad de la evidencia digital, es otro factor relevante para asegurar que las pruebas recopiladas sean confiables y la admisibilidad de la misma.

La confiabilidad nos dice si efectivamente los elementos probatorios aportados vienen de fuentes que son creíbles y verificables, y que sustentan elementos de la defensa o del fiscal en el proceso que se sigue. En la fase para identificar la evidencia con la realización de fotografías y filmaciones en la escena del hecho, levantamiento de elementos informáticos involucrados se garantiza la confiabilidad de la evidencia digital, pues es posible relacionar a la evidencia digital con el incidente ocurrido.

En la fase para recopilar la evidencia digital la extracción original de datos (copia bit a bit) y la obtención de los valores hash con herramientas forenses (con licencia) diseñadas con la finalidad de precautelar la confiabilidad de la evidencia digital, se evita todo tipo de susceptibilidades, éstas herramientas forenses también son utilizadas en la fase para analizar la evidencia digital y al ser con licencia, no existe ninguna duda sobre las herramientas utilizadas.

En el procedimiento para que la evidencia digital sea permitida legalmente se respalda el concepto de confiabilidad con la presencia del fiscal en la escena del hecho; anotando en el cuaderno de investigación lo que se realiza y la constancia en

el acta de solicitud forense con la firma de todos los participantes y los testigos de actuación.

Por todo lo explicado, el método de análisis informático forense garantiza la confiabilidad de la evidencia digital, de tal afirmación obtenemos la siguiente premisa:

q = La evidencia digital es confiable

3.3.1.3 Suficiencia

La suficiencia de la evidencia o más bien, la presencia de toda la evidencia es necesaria para adelantar el caso. Esta es una característica, que igual que las anteriores, es factor crítico de éxito en las investigaciones en procesos judiciales. Frecuentemente la falta de pruebas o insuficiencia de elementos probatorios ocasiona el retraso o terminación de procesos que podrían haberse resuelto.

En este sentido, los abogados reconocen que mientras mayores fuentes de análisis y pruebas se tengan, habrá posibilidades de avanzar en la defensa o acusación en un proceso judicial.

En la fase para identificar la evidencia a secuestrar, se busca identificar la mayor cantidad de evidencia pero que sea relevante al incidente, para que ésta pueda ser adquirida y de ésta forma las pruebas presentadas sean suficientes.

En la fase para recopilar la evidencia digital, se toma en cuenta que no se espera que toda la información que se adquiera deba ser admisible como evidencia, pues mucha de esta información será utilizada para, a través de ella, descubrir evidencia aceptable, es por eso que se trata de adquirir la mayor cantidad de evidencia confiable de una escena del hecho bajo la supervisión y autorización de las autoridades competentes (Juez o Fiscal), para así poder mostrar el escenario completo, y no una perspectiva de un conjunto particular de circunstancias o eventos.

En el procedimiento para que la evidencia digital sea permitida legalmente, esta evidencia es suficiente siempre que cumpla la legalidad en la obtención de la misma, puesto que al ser tachada de ilegal automáticamente queda anulada.

Por tal motivo el método de análisis informático forense garantiza la suficiencia de la evidencia digital, de ésta afirmación obtenemos la siguiente premisa:

q = La evidencia digital es suficiente

3.3.1.4 Conformidad con la legislación vigente en nuestro país

En el procedimiento para que la evidencia digital sea permitida legalmente , se da a conocer la normativa sobre la cual debemos basarnos para aplicar éste método de análisis informático forense, dicho procedimiento se rige en el Código Penal de Bolivia (Art. 363 Bis y 363 Ter), Nuevo Código de Procedimiento Penal de Bolivia y en la Nueva Constitución Política del Estado recientemente promulgada, es oportuno dar a conocer que nuestra legislación no tiene una normativa específica para garantizar que se cumplan las disposiciones legales con la finalidad de que la evidencia digital sea admisible.

Considerar que cuando se tiene acceso a la evidencia digital por medios no autorizados, las mismas son tachadas de ilegales y no existen vías para probar su autenticidad, confiabilidad y suficiencia.

La evidencia debe ser obtenida de manera legal, es por eso que se hace tanto énfasis en contar desde el principio con la orden judicial o requerimiento de un fiscal antes de empezar con la aplicación del método de análisis informático forense.

Además los procedimientos para identificar la evidencia a identificar, recopilar, preservar y analizar la evidencia digital están enmarcados en el "Procedimiento para

que la evidencia digital sea permitida legalmente", púes todo lo que se realice con la evidencia digital debe estar en conformidad con la legislación vigente de nuestro país; de esta forma cumplir con el cuarto concepto requerido para la admisibilidad de la evidencia digital.

Por tal motivo, el método de análisis informático forense garantiza que la evidencia digital esté en conformidad con la legislación vigente en nuestro país, por tal afirmación obtenemos la siguiente premisa:

r = La evidencia digital está en conformidad con la legislación vigente en nuestro país

Por los planteamientos expuestos anteriormente, se afirma que el análisis informático forense para la recopilación confiable de datos y evidencias digitales, garantiza de la evidencia digital la autenticidad, suficiencia y conformidad con la legislación vigente en nuestro país, de ésta afirmación obtenemos:

p = La evidencia digital es auténtica
q = La evidencia digital es confiable
r = La evidencia digital es suficiente
s = La evidencia digital está en conformidad con la legislación vigente en nuestro país

$$(p \wedge q \wedge r \wedge s) \rightarrow t$$

Donde *t = Garantiza la recopilación confiable y esta es admitida en un proceso jurídico*

Una regla de inferencia es ***confiable*** si las conclusiones son verdaderas en todos aquellos casos –estados– donde todas las premisas también son verdaderas.

Por la Regla de Inferencia del Modus Ponens del Razonamiento Deductivo Válido, tenemos:

(p ^ q ^ r^ s): // Del método de análisis informático forense de ésta tesis

(p ^ q ^ r^ s): → t

---

t // garantiza la admisibilidad de la evidencia digital

Para nuestro caso u = (p ^ q ^ r^ s):

Para probar la confiabilidad puede construirse una tabla de verdad, probándose que para todos los modelos en los que las premisas son verdadera, las conclusiones también lo son.

Modus Ponens: u

u→t

---

t

Tabla de Verdad:

u	t	[u	^	(u→t)]	→	t
V	V	V	V	V	V	V
V	F	V	F	F	V	F
F	V	F	F	V	V	V
F	F	F	F	V	V	F
		(1)	(3)	(2)	(5)	(4)

Por lo tanto, como (5) es una tautología, queda demostrado que éste razonamiento es válido. Con lo cual se concluye que el método de análisis informático forense garantiza la recopilación confiable de datos y evidencias digitales en situaciones jurídicas en nuestro país, púes si se maneja debidamente la evidencia digital de manera que se mantenga su autenticidad, suficiencia y conformidad con la legislación vigente en nuestro país, la evidencia digital es confiable como elemento probatorio dentro de un proceso legal.

CAPITULO IV

CAPITULO 4

CONCLUSIONES Y RECOMENDACIONES

En éste capítulo se muestran las conclusiones y recomendaciones que pueden servir para continuar en un futuro esta línea de investigación y desarrollo.

4.1 CONCLUSIONES.

Se desarrolló el método de análisis informático forense con el cual se llega a la obtención del material incriminatorio para su debida sanción de acuerdo a las leyes de nuestro país.

- Se realizó un estudio de las diferentes herramientas desarrolladas para el análisis informático forense.
- Se desarrolló procedimientos para la identificación, recopilación preservación, análisis de la evidencia digital para lo cual ayuda a esclarecer actos delictivos
- El método planteado facilita su mejor desempeño, a los seguidores de esta área.

El conocimiento de informática forense es relativamente bajo por parte de las entidades involucradas en el esclarecimiento de delitos informáticos.
Los elementos que se toman en cuenta para la confiabilidad de la evidencia digital presentada en un juicio son:

- ✓ El perito informático debe tener conocimiento amplio del tipo de delito que se está analizando para saber qué tipo de información está buscando, donde encontrarla y como analizarla.

- ✓ A juicio de abogados y jueces existe desconfianza ante la validez y confiabilidad de la evidencia digital, porque consideran que es una prueba fácil de manipular y

no se puede detectar a simple vista si ha sido contaminada o no. La consecuencia de no tener confianza en la evidencia presentada es que no será aceptada por el juez en un juicio, provocando de esta manera impunidad en casos de delitos informáticos

4.2. RECOMENDACIONES

Profundizar temas referentes a informática forense, pues siendo ésta una nueva disciplina hace falta investigar y ampliar nuestros conocimientos en ésta área.

El requerimiento de seguridad de mayor prioridad para el equipo de seguridad y auditoría fue la disponibilidad de procesos formales y la capacitación en cuanto a la identificación de vulnerabilidades análisis forense y atención a incidentes de seguridad, debido a que necesitan estar capacitados y contar con los recursos necesarios para cumplir con sus actividades diarias.

Es fundamental para el éxito de la metodología que tanto los administradores como el equipo de seguridad participen en la investigación con la finalidad de lograr el compromiso, respaldo, credibilidad, colaboración y cumplimiento de los procesos relacionados con el análisis forense.

El método podría utilizarse en proyectos en donde se desee determinar las vulnerabilidades y mitigación de riesgos a los que están expuestos ciertos recursos.

Además se sugiere gestionar la creación de una nueva mención dentro del pensúm de la Carrera de Informática, pues es necesaria la formación de profesionales en el área de Informática Forense, ya que hasta la fecha en nuestra carrera se opta al Título de Licenciatura en Informática con Mención en Ingeniería de Sistemas Informáticos y con Mención en Ciencias de la Computación, sería un gran avance que se pueda optar al "Titulo de Licenciatura en Informática con Mención en Informática Forense".

BIBLIOGRAFÍA

[Access Data, 2008] Access Data: Forensic Toolkit Consultado el 9 de Septiembre de 2011 en la WWW: www.accessdata.com/media/es_MX/print/brochures/AD.ProdBrochure.es_MX.pdf

[Cano, 2003a] Cano, Jeimy J. (2003). Admisibilidad de la Evidencia Digital: Algunos elementos de revisión y análisis. Revista de Derecho Informatico Alfa-Redi. Consultado el 19 de julio de 2011 en la WWW: http://www.alfa-redi.org

[Cano, 2003b] Cano, Jeimy J. (2003). Introducción a la Informatica Forense. Revista de Derecho Informatico Alfa-Redi. Consultado el 28 de octubre de 2011 en la WWW: http://www.alfa-redi.org

[Caracciolo] Caracciolo, Claudio B. (n.d.). I Jornada: "Tecnología, Integración.. … ¿Seguridad?". Consultado el 14 de octubre de 2011 en la www.ona.gob.ve/Vision360/Presentaciones/CCaracciolo.pdf

[Casey, 2001] Casey, E. (2001) Handbook of Computer Crime Investigation. Academic Press.

[Código Penal, 1999] Ley del Código Penal. Ley No. 1970, Ley Del 25 De Marzo de 1999, Hugo Banzer Suarez, Presidente de la Republica de Bolivia.

[Dávila, 2006] Dávila, Gladys (2006). El Razonamiento Inductivo y Deductivo Dentro del Proceso Investigativo en Ciencias Experimentales y Sociales. Revista de Educación Laurus, vol 12, 184 - 189.Universidad Pedagógica Experimental Libertador Caracas de Caracas – Venezuela. Consultado el 15 de septiembre de 2011en la WWW: http://redalyc.uaemex.mx/redalyc/pdf/761/76109911.pdf

[Guidance Software, 2008] Guidance Software Consultado el 9 de septiembre de 2008 http://www.guidancesoftware.com/products/ef_index.asp

[IOCE, 2000] IOCE. (2000) Elements for testing of internet investigators. IOCE – International Organization on Computer Evidence. IOCE 2000 Conference. http://www.ioce.org/.

[Inza, 2006] Inza, Julián(2006).Consultado el 9 de septiembre de 2011 en WWW: inza.wordpress.com/2006/11/26/herramientas-de-informatica-forense-para-memorias-usb/ - 96k

[Ley Orgánica Ministerio Público, Bolivia] Ley Orgánica del Ministerio Público. Ley Nº 2175. Honorable Congreso Nacional de Bolivia.

[Mckemmish, 1999] Mckemmish, R (1999). What is forensic computing?. Australian Institute of Criminology. Issues and Trenes in crime and criminal justice. No. 118.

[Reino, 2007] Reino, Alfredo (2007, octubre). Informática Forense (II). Práctica de análisis forense. Consultado el 10 de agosto de 2011 en la WWW: http://www.areino.com/forensics-2/

[Restrepo, 2007] Restrepo, Ana María (2007, junio). Computación Forense, Análisis de "Cadáveres" Virtuales. Comunnity CXO. Consultado el 9 de septiembre de 2011 en la WWW: http://www.dragonjar.org/computacion-forense-analisis-de-cadaveres-virtuales.xhtml

[Rojo, 1996] Rojo, Armando O. (1996) Lógica- Razonamiento Deductivo Válido, Algebra I-18ª. ed.- Buenos Aires: El Ateneo

[Rosales, 2008] Rosales, Guido E. (2008, septiembre) Ingeniero de sistemas y

Master en Ciencias de la Ingeniería, especialista en seguridad informatica.

Seminario INFOFOR sobre Informatica Forense , La Paz – Bolivia, 19-20

septiembre, (paper).

[Sommer, 1995] Sommer, P. (1995) Forensic Computing – CSRC Research Project. http://csrc.lse.ac.uk/People/sommerp/forensic.htm

[Torres et al., 2006] Torres, Daniel A.; Cano, Jeimy J. y Rueda, Sandra J. (2006, noviembre). Procedimiento forense para el manejo de investigaciones.

Evidencia digital en el contexto colombiano. Revista ACIS. Consultado el 14 de septiembre de 2011 en la WWW: http://www.acis.org.co/index.php?id=856

[Velásquez, 2008] Velásquez, Andrés (2008, junio). Conversaciones e ideas sobre negocios y nuevas tecnologías. Entrevista sobre computo forense. Radio Eón 4.5 Frecuencia Cero por Antonio Quirarde. México.

[Wikipedia, 2008] Wikipedia (2011).Delitos Informáticos. Consultado el 5 octubre de 2011 en la WWW: http://es.wikipedia.org/wiki/Delitos_inform%C3%A1ticos

ANEXOS

Anexo A

Análisis Informático forense Fraude efectuado por manipulación informática

Fase de Identificación de la evidencia

-Una vez que se haya notificado la denuncia del caso a investigar, para este caso se requiere la presencia del fiscal e investigadores especializados en el área.

- Asegurar la escena del crimen
- Se llena en el formulario de Solicitud forense, todo lo que esté involucrado con la escena del delito en este caso cajero automático.
- Disco duro
- Memoria RAM
- Solicitar video grabación del video de seguridad

Fase de recopilación de la evidencia

Utilizando wantes de látex componentes

Cartones, bolsas antiestáticas

- Se recopila el Disco Duro altamente voltil
- La memoria RAM medianamente volátil (Procesos en ejecución)
- Memoria de video

Fase de Preservación de la evidencia

Para determinar la autencidad del documento, es necesario :

- Hacer copias de la evidencia recopilada para no alterar el original y mantener su

integridad.

- El valor hash obtenido también debe registrarse en el formulario de adquisición de evidencia digital, para demostrar la integridad y autenticidad de la evidencia digital.
- Precintar cada evidencia e inclusive la copia para que no exista susceptibilidad de desconfianza al momento de analizar la evidencia
- La cadena de custodia es esencial, pues en caso de adulteración de la prueba, nos permitiría investigar las causas, y posibles responsables
- La cadena de custodia deberá contener información sobre el dispositivo incautado, número de serie, fabricante, y una descripción detallada acerca de quienes han tenido en su poder la evidencia, sus razones, procedimientos, y los detalles sobre la fecha y la hora exacta de todos estos sucesos. Todo esto detallar en el acta de Identificación y Cadena de Custodia.

Fase de Análisis de la evidencia

Una vez realizado las fases anteriores se procede al análisis, para el dicho caso se sigue los siguientes pasos.

1. *Imagen de datos*

En este caso fue proveída junto a su marco circunstancial.

2. *Verificación de integridad de la imagen*

Previamente se realizo la verificación de integridad del archivo proveído con el caso, es importante tener en cuenta que la verificación de integridad se hizo frente a una imagen y no contra la fuente original.

Creación de una copia de la imagen suministrada

En un análisis de datos nunca se debe trabajar sobre la imagen original suministrada sino sobre una copia.

3. *Aseguramiento de la imagen suministrada*

Como se trabaja con EnCase este software genera un archivo de trabajo. Debido a que se está trabajando sobre una copia segura de solo lectura, se puede asegurar la imagen guardando el original en un lugar seguro o en un dispositivo de almacenamiento electrónico, la cual garantiza que la imagen suministrada no sufra

ningún tipo de alteración, con el fin de conservación de la cadena de custodia y del mantenimiento de la validez jurídica de la evidencia.

4. *Revisión antivirus y verificación de la integridad de la copia de la imagen*

Para este caso se realizara una examinación dd Linux, para después la revisión antivirus sobre Windows, usando Norton antivirus.

Posteriormente el cálculo del compendio criptográfico del archivo para compararlo con el compendio inicial de la imagen obtenida del caso.

5. *Identificación de las particiones actuales y anteriores (las que sea posible recuperar)*

Según Guidance Software Encase identifica las particiones del disco por medio de la búsqueda y en este caso solo identifico ninguna partición en el disco, por lo tanto podemos asumir que solo tiene una partición.

6. *Detección de información en los espacios entre las particiones*

No existe espacio entre particiones que pueda ser analizado

7. *Identificación del sistema de archivos*

Ya que EnCase busca automáticamente el sistema de archivos de la imagen y por esta razón pude mostrar d manera ordenada sus archivos, se debe realizar una búsqueda en el boot de la imagen para identificar el tipo de sistema de archivos.

8. *Recuperación de los archivos borrados*

En la recuperación inicial de la imagen, encase reconoce alnos clusters no asignados y archivos eliminados, mostrándolos en el árbol de archivos.

9. *Recuperación de información escondida*

En esta etapa se debe examinar exhaustivamente los campos reservados en el sistema de archivos y los espacios etiquetados como dañados por el sistema de archivos.

Al igual que en la etapa 9, los archivos protegidos también se tendrán en cuenta durante la etapa de análisis de este tipo de archivos.

10. Identificación de archivos existentes

Seguidamente se clasifican los archivos restantes entre protegidos y no protegidos, donde estos últimos harán parte de los archivos potencialmente analizables, mientras los primeros harán parte en la etapa de análisis de archivos protegidos.

11. Identificación de archivos protegidos

Esta es la tapa e consolidación de archivos protegidos identificados en las etapas anteriores. Durante esta fase se pretende descifrar o romper tal protección en estos archivos, con el fin de adicionarlos al conjunto de archivos potencialmente analizables. Los archivos cuya protección no pudo ser vulnerada formaran parte del conjunto de archivos sospechosos.

12. Consolidación de archivos potencialmente analizables

Durante esta etapa se reúnen todos los archivos encontrados durante las fases de recuperación de archivos borrados, recuperación de información escondida, identificación de archivos existentes e identificación de archivos protegidos.

13. Determinación del sistema operativo y las aplicaciones

Al terminar el sistema operativo y las aplicaciones instaladas, se está en la capacidad de obtener la lista de compendios criptográficos de los archivos típicos del sistema operativo y de las aplicaciones, para verificar posteriormente la integridad de estos archivos de encontrarse en la imagen sometida a análisis.

14. Filtrado basado en archivos buenos conocidos

Con la lista de compendios criptográficos obtenida en el paso anterior, se procede a verificar la integridad de los archivos en la imagen que aparecen en tal lista. Si dicha comprobación es exitosa, este se considera "bueno" y por lo tanto, es descartado el proceso de análisis.

15. Consolidación de archivos sospechosos

Como resultado del filtrado de "buenos" conocidos se obtiene un conjunto de archivos susceptibles a análisis, este conjunto se llamará archivos sospechosos.

16. Primera clasificación

En este caso uno de los archivos con mas prioridad es uno de los archivos Word que se encuentra eliminado, aunque también se debe realizar un análisis de firmas de otros archivos existentes.

EnCase no arrojo ninguna inconsistencia entre los archivos y su extensión,, pero se identificó manualmente que el contenido de dos archivos no correspondía a su extensión coverpage.jpgc y shedule visits.exe

17. Segunda clasificación

Durante esta fase se analiza el archivo de Word identificando el paso de recuperación de archivos borrados, lo que revela los datos concretos relevantes a la investigación.

18. Analizar los archivos

EnCase proporcionó información suficiente para determinar la cantidad real de clusters del archivo y poder reconstruirlo.

19. Archivos comprometidos con el caso

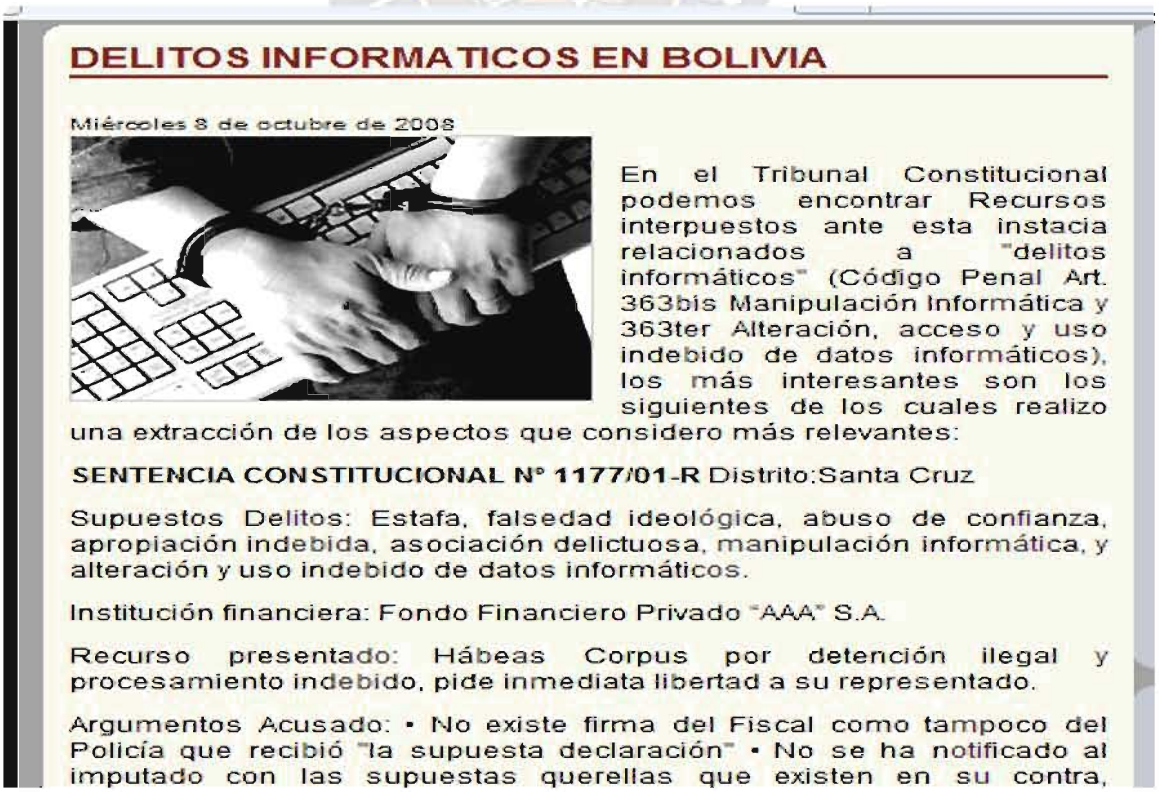
Coverpage.jpgc, Schedule Visits.xls, jimijungle.doc

20. Obtención de línea de tiempo

En este caso no es necesario hacer un alinea de tiempo ya que el caso se resolvió completamente mediante los archivos encontrados y sus relaciones.

Fase de Generación del informe

Se elabora el informe de hallazgos, que contiene una descripción detallada de los hallazgos relevantes al caso y la forma como fueron encontrados, apoyándose en la documentación continua de la aplicación técnica.



DELITOS INFORMATICOS EN BOLIVIA

Miércoles 8 de octubre de 2008

En el Tribunal Constitucional podemos encontrar Recursos interpuestos ante esta instacia relacionados a "delitos informáticos" (Código Penal Art. 363bis Manipulación Informática y 363ter Alteración, acceso y uso indebido de datos informáticos), los más interesantes son los siguientes de los cuales realizo una extracción de los aspectos que considero más relevantes:

SENTENCIA CONSTITUCIONAL N° 1177/01-R Distrito:Santa Cruz

Supuestos Delitos: Estafa, falsedad ideológica, abuso de confianza, apropiación indebida, asociación delictuosa, manipulación informática, y alteración y uso indebido de datos informáticos.

Institución financiera: Fondo Financiero Privado "AAA" S.A.

Recurso presentado: Hábeas Corpus por detención ilegal y procesamiento indebido, pide inmediata libertad a su representado.

Argumentos Acusado: • No existe firma del Fiscal como tampoco del Policía que recibió "la supuesta declaración" • No se ha notificado al imputado con las supuestas querellas que existen en su contra,

ANEXO B

HERRAMIENTAS FORENSES

Las herramientas informáticas, son la base esencial de los análisis de las evidencias digitales en los medios informáticos. Sin embargo, éstas requieren de una formalidad adicional que permita validar tanto la confiabilidad de los resultados de la aplicación de las mismas, como la formación y conocimiento del investigador (informático forense) que las utiliza.

Características de las herramientas de recolección forenses [Torres et al., 2006]

Las características técnicas mínimas que deben cumplir las herramientas forenses para que la evidencia recolectada y/o analizada por ellas sea confiable son las siguientes:

- Manejar diferentes niveles de abstracción: dado que el formato de la información en su nivel más bajo es difícil de leer, la herramienta debe interpretar la información y ofrecer acceso en diferentes niveles.
- Deben tener la capacidad de extraer una imagen bit a bit de la información. Todo byte debe ser copiado de la fuente, desde el comienzo hasta el final de ella sin importar si hay fragmentos en blanco.
- Deben tener un manejo robusto de errores de lectura. Si el proceso de copia falla al leer un sector del medio fuente, se debe marcar en el medio destino un sector del mismo tamaño y en la misma ubicación que identifique el sector que no pudo leerse, adicionalmente estas fallas deben ser documentadas.
- La aplicación no debe cambiar de ninguna manera el medio original, debe tener la habilidad de realizar pruebas y análisis de una manera científica. Estos resultados deben poder ser reproducibles y verificables por una tercera persona.

Las herramientas utilizadas actualmente en informática forense están cumpliendo una función importante para esclarecer los hechos ante incidentes informáticos, a continuación se dan a conocer algunas herramientas que son utilizadas en la

aplicación de la informatica forense [Fernández, 2004]. El uso de herramientas para tratar la evidencia es tanto en ámbito de hardware y software: HARDWARE Se mencionan equipos especializados en identificación biométrica como en captura de evidencias. • Como Identificación biométrica: Usados para autenticar la identidad de un usuario a través de un atributo o rasgo único. Esto generalmente implica el uso de un lector. Algunos tipos: a)Huella Digital b)Análisis de palma c)Iris, retina d)Rostro e)Reconocimiento de Voz • Como captura de evidencias: Brindan la posibilidad de recopilar evidencias (copias) preservando las características y detalles de la evidencia original. Por ejemplo tenemos:

a) DIBS RAID:

Dispositivo de hardware de una sola vía, para realizar copias forenses de disco a disco. Es necesario abrir el computador y manipular el disco sospechoso.

b) DIBS PERU

Realiza las copias en cartuchos ópticos, que permite hacer copias sin necesidad de conectar directamente el disco sospechoso al dispositivo. No se manipula directamente el disco duro sospechoso.

c) ICS Products

Estos dispositivos duplican el disco duro dañado y trabajan con éste. Al analizarlo, a través de un "booteo" se acceden a los datos. • NOTA: Un caso especial, que no encaja en los casos anteriores, es para una herramienta que controla y monitorea el uso de una computadora, se trata del KeyLogger. El Keylogger viene a ser una aplicación que almacena las pulsaciones sobre el teclado, siendo ésto guardado en un archivo o en mail, con información sobre el proceso, hora , fecha, mensajes de la aplicación, etc. El usuario no se dará cuenta del uso de esta herramienta, ya que trabaja en modo oculto. SOFTWARE

Existe software forense que opera creando una copia de respaldo de la información a analizar. Tenemos por ejemplo:

a) EnCase Forensic [Guidance Software, 2008]:

Software líder en el mercado, de mayor uso en el ámbito de análisis forense. EnCase Forensic le proporciona las herramientas para investigar y documentar con éxito muchos delitos locales internos (pornografía infantil, violencia doméstica, acoso, drogas, apuestas y robo de identidad), sin omitir evidencia informática valiosa o tener que esperar laboratorios con trabajo atrasado. La solución permite a los examinadores investigar la evidencia dentro de una sola interfaz gráfica, mediante el uso de un grupo de herramientas, que reduce drásticamente el tiempo que los investigadores emplean en casos individuales. Desarrollado por expertos en análisis forense penal, EnCase Forensic cuenta con la aprobación de tribunales de justicia de todo el mundo. El software sigue siendo la herramienta elegida por el FBI, el Departamento de Seguridad Nacional de Estados Unidos (US Department of Homeland Security), el Departamento de Defensa de Estados Unidos (US Department of Defense), New Scotland Yard y miles de laboratorios criminalistas y agencias encargadas del cumplimiento de la ley en todo el mundo. EnCase Forensic permite que los investigadores manejen fácilmente grandes volúmenes de evidencia informática al visualizar todos los archivos relevantes, incluidos los archivos "eliminados", los espacios muertos de los archivos y los espacios no designados.

Además proporciona las adquisiciones de medios con más validaciones de la industria. La solución crea un duplicado binario exacto de la unidad o disco original y luego lo verifica al generar valores hash MD5 para archivos de imágenes relacionados. Además, EnCase asigna valores de control de redundancia cíclica a los datos a fin de revelar las instancias en que las pruebas se modificaron forzosamente o se alteraron de alguna manera. Este enfoque fue validado por el Instituto Nacional de Normas y Tecnología (National Institute for Standards and Technology, NIST) y resistió numerosos cuestionamientos por parte de los tribunales de justicia.

Características de EnCase:

- Útiles vistas de gráficos

Vistas de línea de tiempo expandida

Muestra de forma instantánea una gran variedad de medios o gráficos informáticos. Es compatible con los formatos ART, BMP, GIF, JPG, PNG y TIFF.

- Vistas de línea de tiempo expandida

Proporciona una vista calendario de todas las actividades en los archivos, que muestra cuándo se crearon los archivos o cuándo se produjo el último acceso o la última escritura. El calendario alterna meses y años para ayudar a los examinadores a ver los patrones de la actividad en los archivos.

- Opciones de adquisición flexibles

Brinda la posibilidad de obtener imágenes de medios con sistemas operativos múltiples, lo que genera flexibilidad y ahorra tiempo en casos de adquisiciones difíciles. La solución admite la obtención de imágenes en Windows, DOS y Linux y presenta diversas opciones de compresión, velocidad y manejo de errores.

- **Informes detallados**

Genera información detallada sobre archivos, carpetas, volúmenes, discos duros y casos específicos. Permite visualizar datos referidos a la adquisición de datos, la geometría de la unidad, las estructuras de las carpetas y las imágenes y los archivos marcados. Exporta informes en formato RTF o HTML.

Genera reporte del proceso, mostrando el caso investigado, la evidencia principal, algunos comentarios, imágenes recuperadas, tiempo en que se realizó la búsqueda.

- **Otras Características**

-Soporte multiplataforma: Windows, Solaris, Macintosh, Linux.

-Crea copias comprimidas de los discos fuente para poder analizarlo, buscarlo y verificarlo.

-Proporciona y documenta eficientemente fechas, horas, registros de accesos, es decir todos los rastros de intervención en un proceso.

-Permite ver archivos borrados, ocultos. EnCase localiza automáticamente y despliega muchos formatos de imágenes, incluyendo las que fueron eliminadas. De todas estas se escogen las imágenes más relevantes para el caso.

b) Forensic Toolkit [Access Data, 2008]:

Es una suite de herramientas para el análisis de las propiedades o especificaciones de ficheros. Examina los ficheros de un disco en busca de actividad no autorizada y los lista por su última fecha de acceso, permitiendo realizar búsquedas en franjas horarias, búsqueda de archivos eliminados y data streams (utilizados para ocultar información en sistemas NT/2K). Obtener atributos de seguridad de ficheros.

Forensic Toolkit de AccessData (FTK) ofrece a los profesionales encargados de controlar el cumplimiento de la ley y a los profesionales de seguridad la capacidad de realizar exámenes forenses informatizados completos y exhaustivos. FTK posee funciones eficaces de filtro y búsqueda de archivos. Los filtros personalizables de FTK permiten buscar en miles de archivos para encontrar rápidamente la prueba que necesita. FTK ha sido reconocida como la mejor herramienta forense para realizar análisis de correo electrónico.

FÁCIL DE USAR

• La tecnología Outside In Viewer de Stellent le permite ver cientos de formatos de archivos

• FTK Imagen le permite navegar rápidamente por las imágenes adquiridas

• Genere registros de auditoría e informes del caso

• Es compatible con Password Recovery Toolkit y Distributed Network Attack

OPCIONES DE BÚSQUEDA AVANZADAS

• Búsqueda en el índice de texto completo suministrada por dtSearch muestra los resultados de búsqueda de texto al instante

• Restauración de datos avanzada para textos de Internet, gráficos, documentos de MS Office entre otros

• Encuentre patrones binarios con Live Search(Búsqueda directa)

• Encuentre archivos importantes rápidamente mediante la creación de filtros de archivos personalizados

REGISTRY VIEWER

• Analice la información de cuenta, como nombres de usuarios y contraseñas, de Internet Explorer, Outlook y Outlook Express

• Abre todas las versiones de archivos de registro de Windows

• Se integra fácilmente con los informes del caso de Forensic Toolkit

ANÁLISIS DE CORREO ELECTRÓNICO Y DE ARCHIVOS ZIP

• Permite: correo electrónico de Outlook, Outlook Express, AOL, Netscape, Yahoo, Earthlink, Eudora, Hotmail y MSN

• Vea, busque, imprima y exporte mensajes y archivos adjuntos de correo electrónico

• Recupere mensajes de correo electrónico borrados parcial o totalmente

• Extraiga datos automáticamente desde archivos comprimidos PKZIP, WinZip, WinRAR, GZIP y TAR

ARCHIVOS Y FORMATOS DE ADQUISICIÓN ADMITIDOS

• Los formatos de archivos incluyen: NTFS, CDFS, UDF, HFS, FAT 12/16/32 y Linux EXT2 & EXT3

• FTK y FTK Imager pueden leer formatos de imágenes de EnCase, SMART, Symantec, Linux DD entre otros

Además que permite: -Análisis de punta, permite descrifrar y crackear password. -El uso de una base de datos para manejar su información obtenida.

c) SafeBACK:

Aplicación usada para crear "imágenes espejo" de disco duro (completo o partición). Algunas características que presenta: -Basado en DOS ya que Windows puede alterar los datos. -Indaga la existencia de archivos ocultos cuando los sectores no presentan semejanza con el enlace de disco duro. -Copia al 100% todas las áreas del disco duro.

El acceso a las memorias USB plantea interesantes retos para los analistas forenses. Herramientas como SafeBack permiten hacer copias exactas de diferentes tipos de memorias (como las que se emplean en las cámaras de fotos digitales) a nivel de bit. Es necesario tener un interfaz fiable para estos tipos de memorias, por lo que es conveniente seleccionar un poco. En el caso de los "lápices" o "llaves" USB el interfaz va incorporado en el dispositivo [Inza, 2006].

DOCUMENTACIÓN