UNIVERSIDAD MAYOR DE SAN ANDRES
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMÁTICA

TESIS DE GRADO

METODO DE ANALISIS FORENSE PARA LA RECOLECCION DE LA EVIDENCIA DIGITAL EN DISPOSITIVOS MOVILES

PARA OPTAR AL TITULO DE LICENCIATURA EN INFORMATICA

MENCION: INGENIERIA DE SISTEMAS INFORMATICOS

POSTULANTE: MIGUEL ANGEL MACUCHAPI PARISACA

TUTOR METODOLOGICO : M.Sc. ALDO RAMIRO VALDEZ ALVARADO

ASESOR : LIC. JAVIER PACHECO REYES

LA PAZ – BOLIVIA

2014

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMÁTICA

LA CARRERA DE INFORMÁTICA DE LA FACULTAD DE CIENCIAS PURAS Y NATURALES PERTENECIENTE A LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICTAMENTE ACADÉMICOS.

LICENCIA DE USO

El usuario está autorizado a:

a) visualizar el documento mediante el uso de un ordenador o dispositivo móvil.
b) copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.
c) copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la referencia correspondiente respetando normas de redacción e investigación.

El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

DEDICATORIA

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

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

A mis hermanos Isabel, René, por el cariño y apoyo incondicional que me brindan.

Miguel Ángel Macuchapi Parisaca

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 siga adelante.

A mis padres, Joséy Asunta, 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 Metodológico M.Sc. Aldo Ramiro Valdez Alvarado, por su confianza, guía y apoyo. Sin su empeño y conocimientos este trabajo no hubiese sido posible.

A mi Asesor Javier Pacheco Reyes, por las sugerencias, correcciones y el tiempo de dicado 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 agradecido.

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 de fraude en los en los dispositivos móviles.

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 describe un Método de análisis Forense que permita la recolección confiable de datos y la evidencia digital, mantener 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, recolección, 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.

INDICE GENERAL

CAPITULO I

MARCO REFERENCIAL

INDICE DE TABLAS

Pag

INDICE DE FIGURAS

Pág.

CAPITULO I

CAPITULO I

1. 1 INTRODUCCION

En el momento en que apareció el teléfono móvil en el mercado español, pocos pudieron imaginar que esta nueva forma de comunicación tendría un impacto tan importante en nuestras relaciones sociales. Probablemente tampoco sospecharon que los adolescentes, e incluso los niños, llegaran a utilizar intensamente está nueva tecnología y que la incluyeran como parte fundamental de su vida cotidiana. Si observamos a nuestro alrededor, tampoco los adultos acabamos de entender cómo, hasta hace relativamente poco tiempo, nuestras vidas transcurrían sin un teléfono móvil en el bolsillo.

Esta nueva plataforma de comunicación e información y las nuevas formas de «ocio de pantalla» quien corpora ha venido desarrollándose en nuestra sociedad a una velocidad sin precedentes. Ha traído con sigo una serie de cambios y consecuencias de carácter multidimensional, que están siendo objeto de atención de los investigadores, especialmente por el impacto que han tenido algunas de sus manifestaciones en la opinión pública. Comportamientos adictivos a esta nueva tecnología entre los más jóvenes, generación de facturas telefónicas astronómicas, o el uso de la cámara o vídeo para captar determinadas escenas ,vienen poniendo de relieve cómo la destreza para su manejo entre los más jóvenes, supera ampliamente alas de sus progenitores. Obliga a reflexionar también acerca de los límites que enfrentan éstos en sus habilidades a la hora de realizar una correcta supervisión de los usos que hacen sus hijos de los teléfonos móviles.

En línea con lo anterior, las posibilidades que se han abierto para las compañías fabricantes y operadoras de estas tecnologías son inmensas, frente a un mercado juvenil que se encuentra suficientemente preparado ante los retos tecnológicos, y que además puede encontrar en el móvil una forma de dar respuesta inmediata a sus exigencias de comunicación, relaciones sociales, información o entretenimiento. Conviene no olvidar que nos encontramos frente a la «generación de lo inmediato» y que el móvil ha ayudado, en cierta manera, a consagrarla. Si necesitan llamar, quieren hacerlo ya; si necesitan ver imágenes de algún acontecimiento, ya sea deportivo, musical, o incluso el final de su serie favorita, desearían verlo ya. Esto nos introduce en problemáticas específicas que van más allá de los análisis tradicionales acerca del uso «comunicativo» del teléfono. La utilización de los teléfonos móviles por parte de jóvenes, adolescentes y niños no se reduce simplemente a la realización de llamadas o envío de mensajes. Aunque ésta haya venido siendo su principal función, la posibilidad de realizar fotografías y vídeo, de conectarse a Internet o de ver televisión

en esta «pequeña pantalla», están siendo ya una realidad, al igual que el poder bajarse determinados contenidos de Internet. Ante esta nueva situación, parece pertinente tratar de plantear nuevas aproximaciones de carácter teórico y analítico al fenómeno, que contemplen las dimensiones individuales y sociales implicadas en sus nuevos usos especialmente por parte de niños y jóvenes teniendo en cuenta que esta tecnología llega, cada vez más, a edades tempranas a este sector de la población, y ha experimentado en los últimos años su consolidación definitiva en nuestra sociedad.

Cabe mencionar también, en este sentido, los estímulos consumistas de diferente tipo relacionados con la telefonía móvil, que se transmiten desde los propios medios de comunicación. Variadas formas de publicidad que invitan a los más jóvenes a descargarse melodías, logos o contenidos musicales, o incluso imágenes y vídeos desde páginas de Internet cuyos contenidos podrían considerarse inapropiados para según qué franjas de edad. Por otro lado, también los medios y la propia red Internet, oferta a los jóvenes la posibilidad de convertirse en emisores o difusores de información, utilizando el móvil como principal herramienta de grabación de acontecimientos. Los móviles se han convertido también en cámaras-testigo que permiten a sus usuarios más jóvenes grabar y difundir escenas de todo tipo, incluso en ocasiones de carácter violento.

Las cadenas de televisión han visto también en los jóvenes un nicho de mercado muy activo en el uso de la telefonía móvil. Son muchos los programas juveniles que incluyen la posibilidad de participar a su audiencia juvenil, enviando comentarios o sugerencias a través de mensajes de telefonía móvil. Los medios tratan de transmitir, de esta manera, la sensación de participación activa, de control de la realidad y de implicación directa con el programa y con todo lo que allí acontece.

Como audiencias consumidoras de tales productos mediáticos, niños y adolescentes acaban siendo en buena medida sus destinatarios finales. Y el precio de tal participación con lleva en ocasiones un gasto familiar que resulta difícil de asumir, ya que los menores no siempre son conscientes del verdadero gasto asociado al uso del teléfono móvil y su impacto real en las economías familiares. Si nos centramos en aquellos riesgos potenciales que entrañan las nuevas capacidades de la tecnología 3G (video llamadas, acceso a Internet de banda ancha, MMS y otras) podríamos agruparlos en las siguientes cuestiones «candentes»:

• Puede fomentar conductas de uso adictivas y/o compulsivas asociadas, además, a un elevado gasto eco nómico como resultado de este uso exacerbado.

• Facilita la grabación y distribución de imágenes susceptibles de ser empleadas en el contexto del acoso escolar (bullying).

• Permite el acceso sin restricción a contenidos audiovisuales no adecuados para la infancia, tales como pornografía, actos vandálicos o violencia extrema.

• Posibilita nuevas vías telemáticas de acceso a los niños por parte de pederastas, facilitando incluso la ubicación exacta de potenciales víctimas mediante el rastreo vía GPS o SBL (sistemas basados en la localización).

• Convierte a niños y jóvenes en receptores de todo tipo de publicidad.

• Posibilita el acceso sin autorización a los datos del terminal, por ejemplo, mediante la intrusión de códigos maliciosos gracias a los cuales un impostor puede enviar mensajes fraudulentos, lo que a su vez podría dar lugar a responsabilidades jurídicas civiles y penales.

La necesidad de comunicación del ser humano lo ha motivado a desarrollar sistemas altamente sofisticados, que incorporan conceptos inalámbricos y de movilidad. El campo de las comunicaciones inalámbricas móviles representadas principalmente por las tecnologías celulares, se ha convertido en uno de los ejes más destacados de las telecomunicaciones a nivel global.

Los dispositivos móviles celulares no son solamente utilizados para tareas ordinarias como recibir y enviar mensajes o llamadas, sino que algunos de ellos proveen las mismas funcionalidades que brinda una computadora de escritorio.

Esto hace que los celulares se conviertan potencialmente en una valiosa fuente de evidencia en un análisis forense.

Por ello se propone y redacta un procedimiento desde el punto de vista técnico y legal, que servirá como guía para realizar un adecuado manejo de la evidencia electrónica y digital en la investigación judicial bajo la cual esté involucrado el teléfono celular.

Paralelamente se analiza el marco legal y regulatorio que existe en el País acerca de evidencia digital, para abordar su importancia, pues actualmente no se tienen leyes claras al respecto.

Estas situaciones potenciales plantean una serie de desafíos a operadoras, creadores del software y productores de contenidos multimedia que es necesario acometer en términos de desarrollo, mejora de los mecanismos técnicos de protección

a la intimidad, autenticación eficaz, encriptado, provisión de un sistema estable y fiable de alerta acerca del consumo de los menores, o desarrollo de sistemas de filtrado de los contenidos por edades.

Hacen conveniente insistir, además, en la necesidad de desarrollar programas educativos que frenen los potenciales riesgos asociados y usos disfuncionales de estas innovaciones tecnológicas.

En perspectiva comparada, las investigaciones realizadas en Gran Bretaña1, con niños de edades comprendidas entre los siete y los once años (n=1.331) mostraron que uno de cada tres niños de este grupo de edad poseía un teléfono móvil, y que cinco de cada siete lo utilizaba para enviar mensajes SMS, lo que re vela cómo incluso los niños preadolescentes se han convertido en avezados usuarios de esta tecnología (Muir, 2005).

También según los datos del Euro barómetro de mayo de 2006, el 70% de los jóvenes europeos entre 12 y 13 años y el 23% de los niños entre 8y 9 años declaraba poseer un teléfono móvil. En algunos países en concreto, como es el caso de Noruega, el 90% de los niños de 10 años tiene un móvil2. Pero se trata de un fenómeno mundial ya que en Japón, por ejemplo, donde los teléfonos móviles con capacidad para la 3G cuentan con una mayor tradición que en el resto del mundo, el 95,2% de los estudiantes de secundaria es propietario de su propio móvil y aproximadamente uno de cada cinco lo utiliza para visitar sitios web de citas –con un incremento en el número de visitas durante el primer semestre de 2006 del 260%o para descargar pornografía.

Hasta el momento se encuentra todavía poco desarrollado en nuestro país, el ámbito de estudio sociológico acerca del impacto de las nuevas tecnologías de la información y comunicación entre los más jóvenes, y los efectos que su utilización está teniendo en sus vidas cotidianas. En concreto, son aún escasos los estudios centrados en el uso e impacto de la telefonía móvil en su desarrollo individual, social y cultural. Sin embargo, empiezan a surgir intereses investigadores de carácter multidisciplinar en este área, que tratan de reflexionar acerca de los problemas y retos que plantea su uso. Las aportaciones teóricas que se presentan a continuación se inscriben dentro de este área de interés, y se fundamentan en la investigación empírica realizada en tal sentido para el Defensor del Menor en la Comunidad de Madrid4. Tratan de contribuir al estudio de esta temática, desarrollando una propuesta de análisis teórico sobre las diferentes dimensiones objeto de estudio, implicadas en el uso de la telefonía móvil por parte de los adolescentes. Este marco teórico pretende ser así, punto de partida para posteriores estudios empíricos relacionados con los

hábitos e influencias de la telefonía móvil, y con la necesaria contribución y concienciación de todos los agentes sociales implicados en el fenómeno.

2 . ANTECEDENTES

Desde mediados de los años setenta del siglo pasado, asistimos en las sociedades industriales avanzadas a un proceso de cambio desde una sociedad industrial a la sociedad de la información y del conocimiento. En la base de este proceso se encuentra lo que algunos autores vienen denominando como la «Tercera Revolución Industrial»; cuyo motor de cambio revolucionario hay que situarlo en una profunda e intensa penetración y aplicación en todos los sectores productivos de las TIC. Se trata de un conjunto convergente de tecnologías relacionadas con la microelectrónica, computación, telecomunicaciones y optoelectrónica (Castells, 1996). El agrupamiento e interrelación de innovaciones asociadas a estos nuevos sistemas tecnológicos ha estado dotado de una amplia adaptabilidad. Los entramados tecnológicos creados con ellas han permitido el crecimiento de nuevas industrias y servicios y, lo que es más importante, el surgimiento de nuevos productos orientados a un consumo de masas con su particular tecnología distintiva–, que están dando lugar a la adopción de nuevos patrones de consumo, hábitos y estilos de vida. Ordenadores personales, cámaras, video cámaras, reproductores de sonido y vídeo digital, videoconsolas, GPS5, televisión digital terrestre, teléfonos móviles o la red Internet… forman parte de los nuevos productos y servicios de esta nueva fase de desarrollo tecnológico, en constante y acelerado progreso.

Estos nuevos fetiches de nuestra sociedad de consumo se han venido integrando en nuestra vida cotidiana durante la última década, contribuyendo a modificar pautas culturales en las sociedades postmodernas.

El teléfono móvil resulta paradigmático a la horade ilustrar el cambio acelerado que venimos comentando.

Nacido tímidamente en Chicago en los años cincuenta, el desarrollo posterior de esta nueva modalidad de teléfono arranca en el mundo occidental aproximadamente hacia 1995, cuando el sistema europeo GSM6 toma el liderazgo sobre otros sistemas americanos y japoneses, y el mercado lo asume y divulga con una fuerza e ímpetu jamás imaginado. Los teléfonos móviles promueven básicamente comunicación rápida, sencilla y directa. Pero el desarrollo de esta tecnología ha obligado a la ingeniería de telecomunicación a dar respuesta rápida a las demandas de los consumidores, como en el caso de la mensajería de texto SMS7 de los últimos años,

obligando a parametrizar nuevos esquemas de redes celulares, nuevos modelos de aparatos, servicios ,aplicaciones y esquemas tarifarios.

A trece años de su implantación, la difusión del teléfono móvil en España abarca prácticamente a toda la población: en febrero de 2008 existían en nuestro país 46 millones de móviles. El número de líneas de telefonía móvil dadas de alta rebasa ya el número de habitantes en España: hay 109 líneas por cada 100 habitantes.
La posesión de un móvil empieza a ser lo que algunos expertos definen como un fenómeno de masas (killer application).

Su adopción se ha producido de forma mucho más rápida a lo que supuso la entrada del televisor o del actual PC en los hogares. Su amplia difusión responde, fundamentalmente ,a las posibilidades comunicativas que brinda –en tiempo real– con independencia del lugar en que nos encontremos. Pero existen también razones estructurales de tipo sociológico, que han venido contribuyendo a su rápido desarrollo como herramienta de comunicación «personal», y que se vinculan conciertas necesidades relacionadas con los profundos cambios que está experimentando nuestra sociedad.

Heurtin (1998) enuncia tres factores presentes en la creciente complejidad de la organización y formas de las interacciones familiares:

• La emergencia de familias mono parentales o recompuestas, particularmente demandantes de lazos telefónicos personalizados, en razón a su estructura «rota»

La «democratización interna» de la familia que acentúa la autonomía de los individuos y favorece la difusión de una telefonía menos colectiva y más personal.

• El alargamiento relativo de la duración de la cohabitación de
los hijos en el hogar paterno, que generala demanda de dispositivos de comunicación individua les que permitan alcanzar una cierta autonomía respecto a los padres.

Se apuntan también otros fenómenos adicionales que han contribuido al crecimiento de la demanda de telefonía móvil entre jóvenes, como puede ser el desarrollo de la cohabitación entre estudiantes y jóvenes graduados que entran al mercado de trabajo, o entre inmigrantes que eligen compartir vivienda y demás gastos relacionados con ella. En este caso, las comunicación es individuales son claramente más frecuentes que las llamadas colectivas –es decir, destinadas al conjunto de los cohabitantés – y el móvil tiende a sustituirá la telefonía fija. Citemos también en este contexto el número cada vez más elevado de adolescentes y jóvenes que pasan sus vacaciones con miembros de su grupo de pares, en cursos en el extranjero o con uno

de sus dos progenitores. Los teléfonos móviles representan en estos casos el canal de «conexión» entre el joven y el resto de la familia.

Niños y adolescentes son fieles usuarios de los productos estrella en el ámbito de las nuevas tecnologías en mayor medida que los adultos (Feixa, González, Martínez & Porzio, 2002). En los últimos años, el uso de Internet y de telefonía móvil ha experimentado entre ellos un crecimiento sin precedentes. Los jóvenes han sido los usuarios más activos (Valor & Sieber, 2004). Por esta razón se les define dentro del sector como usuarios intensivos (heavy users): no sólo tienen móvil sino que lo utilizan constantemente.

La mayor parte de los investigadores sociales vincula el amplio desarrollo del teléfono móvil entre los más jóvenes basándose en los conceptos sociológicos de grupo y de relaciones primarias, que provocan entre adolescentes dos urgentes necesidades, de identidad y de comunicación. De identidad, porque necesitan definir y sentir quiénes son: jóvenes entre jóvenes, en un espacio propio intransferible, privado y se parado de los padres. La necesidad de comunicación va encaminada a construir su entramado social de valores, normas y comportamientos, en definitiva, su (sub)cultura.

Los adolescentes necesitan construir su identidad con una mirada endogámica, relacionándose, comunicándose y cerrándose en su micro-mundo juvenil y este hecho, por otro lado, representa una oportunidad de mercado en nuestra sociedad de consumo(Battle, 2007).

Por otra parte, también hay que atender al hecho de que la actual generación de niños y adolescentes es la primera que ha sido educada en la sociedad digital: es la denominada «Generación red» (Tapscott, 1998).

Se trata de la primera generación que llegará a la mayoría de edad en la era digital. Los actuales niños y adolescentes están siendo preparados para usar todas las potencialidades de las nuevas tecnologías. Son los mejor preparados para adaptarse a los cambios, para afrontar el futuro sin los prejuicios y aversión tecnológica de sus progenitores. Representan el grupo de edad con mayor acceso a ordenadores e Internet, y la mayor parte de sus integrantes viven rodeados de bites, chats, e-mails, webs y blogs. Desde que tienen uso de razón han estado rodeados de instrumentos electrónicos desde tamagochis y video juegos a relojes digitales– que han contribuido a configurar su visión dela vida y del mundo que les rodea. Su definición como «Generación @» también pretende recoger es tas tendencias de cambio que les afectan y que tienen que ver, fundamentalmente, con sus habilidades, disposición y acceso casi universal a las nuevas tecnologías dela información y comunicación (Opas chows ki, 1999).

El nuevo modelo de adolescencia actual habría determinado la emergencia de mundos virtuales como las comunidades de internautas o la configuración de redes de adolescentes a escala planetaria. Esta situación estaría propiciando un modelo de inserción virtual delos adolescentes en sociedad. El paso de un modelo basado en la cultura visual, a otro basado en la cultura multimedia, promovido por el uso de In ter net, cuyas consecuencias sobre la vida adulta aún es tán por determinar.

Propuesta para el estudio de las dimensiones y funciones del teléfono móvil en adolescentes

Hemos descrito hasta aquí el nuevo contexto social y tecnológico en donde se insertan las vivencias de los adolescentes españoles en la actualidad. En este apartado nos ocupamos de describir cómo podemos analizar, de forma típico-ideal, los usos del teléfono móvil en esta franja de edad.

La adolescencia es aquel período del ciclo vital, en el cual el niño aprende un conocimiento funcional del modo de actuar como actor social independiente. Esto se traduce, tanto en la adquisición de varios tipos de conocimientos teórico-prácticos y técnicos, como en la exigencia a que empiece a desarrollar el rol correspondiente para ser considerado un adulto. Los conocimientos específicos que acompañan esta socialización temprana inculcada desde la familia y la escuela deben incluir básicamente:

• La formación en el respeto a los derechos y libertades, y en el ejercicio de la tolerancia dentro de los principios democráticos de convivencia.

• El respeto a la pluralidad.

• El aprecio a los valores básicos que rigen la vida.

• La adquisición de habilidades que le permitan desenvolverse con autonomía en los ámbitos familiar y doméstico, en el grupo de pares, y en grupos sociales más amplios.

• El desarrollo del sentido crítico.

• El comportamiento con espíritu de cooperación, responsabilidad moral y solidaridad, respetando la no discriminación entre las personas.

• La valoración de diferentes hábitos sociales.

• La comprensión de la economía, y de la economía familiar y personal en particular.

• El desarrollo de estrategias para la negociación con individuos y grupos.

• El conocimiento de cómo interactuar y usar las TIC.

Es durante la adolescencia cuando el niño empieza a ensayar su autonomía a través de sus amistades, tratando de construir su propia vida emancipándose gradualmente de sus padres. Por esa razón en el adolescente los amigos adquieren un protagonismo central, trascendiendo a cualquier otro tipo de relación en importancia.

Hay una insistencia muy fuerte en el grupo de iguales como grupo de referencia, y el papel de los padres es reemplazado progresivamente por la orientación hacia el grupo de iguales.

Por otra parte, un móvil puede ser –y de hecho loes en algunos modelos comerciales una agenda electrónica, un reloj, un despertador, un calendario, una calculadora, un conversor de unidades, un reproductor de música, vídeos y televisión, una consola de juegos, una cámara o videocámara digital, una agenda electrónica, un álbum de música, fotos, vídeos y mensajes, un contestador automático, un pequeño ordenador, un GPS o localizador, y un terminal de navegación por Internet, además de un teléfono. Sus múltiples utilidades actuales son un dato previo a tener en cuenta, si queremos realizar un correcto análisis acerca de las consecuencias en los adolescentes de sus potenciales usos.

Desde esta premisa vamos a entenderlo en su dimensión instrumental, como un instrumento multiuso de comunicación, expresión, ocio e información, dotado de un elevado componente de autonomía. Como« instrumento a la carta» que cada cual utiliza y configura en función de sus intereses, objetivos y necesidades puntuales, permite estar localizado, hablar, jugar y recrearse en sus funciones cuando se quiera, con quien se quiera y donde se quiera, siempre que se disponga –en función del uso, de batería, cobertura o saldo. Sus numerosas funciones no deben hacernos perder de vista, sin embargo, que se trata originalmente y de forma primaria de un dispositivo de comunicación. De manera que dentro de su dimensión instrumental se hace preciso diferenciar entre su función comunicativa básica, y su función lúdico-expresiva. La primera hace referencia a su carácter bidireccional e interactivo de comunicación a través dela voz, mensajes o tonos, de informaciones, sentimientos o decisiones. La segunda se relaciona con sus otras utilidades, relacionadas con usos recreativos vinculados al ocio, el juego y expresiones creativas (fotos, vídeos, pero también mensajes), como acciones intencionales del individuo a través de las que trata de dar respuesta a necesidades lúdicas, artísticas, o de singularidad y originalidad.

Ahora bien, vamos a partir de la hipótesis que el uso y la elección del teléfono móvil por parte de los jóvenes no es puramente funcional ni racional ligado a la relación calidad/precio del aparato, sino que está relacionada con una dimensión simbólica que tiene que ver con su apariencia, sus prestaciones, su marca y su coste.

Al igual que la ropa, el corte de pelo, tatuajes, piercings u otras modalidades de expresión corporal y objetos de consumo, es probable que cada tipo de móvil esté siendo asociado a una serie de significados, códigos y valores, que contribuyen a conferir simbólicamente a su propietario una imagen concreta valorada dentro de su subcultura.

Parece plausible que, como otras mercancías dirigidas a un consumo os ten toso, el móvil sea un instrumento simbólico, que refiere y transmite significados acerca de las características personales y posicionamientos sociales del individuo, de su grupo de referencia, y sobre las ideas que éste se hace de sí mismo y de los demás.

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 "que", "quien", "cuando" ,"como", y en algunos casos ,el "porque" de un incidente.

Para ello realizar el análisis de recolección de la evidencia será dar la importancia de poder examinar detalladamente la información que sea relevante y que pueda estar almacenada , escondida, cifrada o suprimida en un dispositivo móvil, la acumulación de evidencias inobjetables irán destinadas al esclarecimiento de problema ilícito para su posterior proceso legal.

3.1. PROBLEMA CENTRAL

A través del tratamiento del análisis, se podrá obtener la importancia, la relevancia y la necesidad de tener técnicas forenses que ayuden a la investigación, desde el punto de vista científico y técnico, con el fin de poder interactuar de una manera más directa con una posible evidencia física del tipo digital, que a su vez se pueden utilizar según la legislación boliviana como elemento probatorio de practica ilícita.

3.2 PROBLEMAS SECUNDARIOS

Como causa al problema será adicionalmente que se presentara:

Algunas variaciones en la estructura y ubicación de los datos y en el sistema incorporado de algunos modelos de teléfonos que son personalizados para los operadores por los fabricantes.

Pero una vez que el investigador forense allá identificado la marca (o fabricante en la mayoría de los casos) y el modelo del ME, por efecto deberá proceder a realizar el análisis.

4. DEFINICIÓN DE OBJETIVOS

Obtener un análisis forense factible que solucione los procesos de respuesta a los incidentes de seguridad y establecer normas a estas de evidencias en los dispositivos móviles.

4.1. 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.

4.2 OBJETIVOS ESPECIFICOS

En definitiva se trata de recoger aquellos elementos fundamentales:

- **Paso I.** Obtener información previa sobre el caso. Antes incluso de iniciar la recogida de evidencias, el analista debe ser conocedor de las circunstancias del escenario en el que se han desarrollado los hechos, así como disponer de la máxima información posible sobre ellos. Para esto es necesario acudir a todos aquellos que

pudieran proporcionarla. La complejidad del escenario determinará también la cantidad de evidencias a recuperar y tratar. Cuanto mayor sea el volumen de información inicial obtenida, menor será el número de problemas posteriores derivados de la falta de datos o de la inconexión de los mismos.

- **Paso II.** Obtención de evidencias. Es determinante la recuperación rigurosa y la firma de las evidencias asociadas a cada caso, generando además los ficheros de cadena de custodia correspondientes. De forma especial en nuestro país, la no alteración bajo ningún concepto de las pruebas y la garantía por lo tanto de su valor pericial son la máxima fundamental a observar en los procesos de recuperación de evidencias. Este mismo concepto deberá regir el almacenamiento seguro de las pruebas recogidas que pudieran posteriormente ser utilizadas en un juicio.

- **Paso III**. Identificar datos relevantes y la línea temporal de la investigación. Es estratégico identificar los datos importantes en función de las circunstancias de cada caso: nombres, direcciones, correos, números de teléfono, ficheros, etc. Con ello se facilitará la posibilidad de realizar búsquedas eficaces. De igual modo, debe definirse la línea temporal que se tendrá en consideración para el desarrollo de la investigación pericial. Esto permitirá articular una investigación basada en un proceso secuencial, manejable y que facilite la elaboración de un informe eficaz.

- **Paso IV.** Ordenar y relacionar los datos obtenidos a partir de las evidencias del caso. Teniendo siempre en consideración la garantía de independencia del perito y la incapacidad para ocultar cualquier dato aunque sea negativo para la parte por la que ha sido contratado. Las conclusiones deben exponerse sin ningún tipo de injerencias si el pericial quiere tener el valor que le corresponde en el juicio. No se debe despreciar tampoco la posibilidad de que pueda realizarse un contra pericial que destape datos que hayan podido ocultarse, con el consiguiente efecto negativo, tanto para la parte como para el propio perito.

- **Paso V.** Generación del informe pericial. El objetivo es construir un informe escrupuloso, técnico pero legible y con unas conclusiones sólidas que permitan arrojar luz sobre el caso. Deberán evitarse las verdades a medias y cualquier apreciación dudosa emitida a través de prejuicios obtenidos en los pasos previos. Como ya se ha expuesto en el capítulo correspondiente, un elemento muy importante del informe consiste en reflejar las garantías observadas en el proceso y que permiten dar absoluta veracidad a las evidencias.

- Paso VI. Práctica de prueba anticipada. Toda vez que el informe esté concluido y se tenga en consideración la posibilidad de llegar a juicio, se deberá aconsejar al abogado, la práctica de la prueba anticipada cuando las circunstancias así lo requieran.

- Paso VII. Asesoramiento técnico. Es necesario apoyar al abogado técnicamente en la estrategia a llevar en el juicio para la defensa de la labor e informe pericial, así como en la preparación de la nota que deberá presentarse para la vista. De igual modo, deberán definirse con antelación aquellas preguntas claves que permitan presentar las conclusiones del informe más importantes.

- Paso VIII. Intervención en la vista judicial. En el juicio, el perito desempeña un papel clave. La otra parte en todo momento intentará desmontar los argumentos técnicos que presente, pero también buscará desacreditar su figura, poniendo en duda su imparcialidad. Sabe que cualquier atisbo de duda en este sentido, provocará que pruebas e informes técnicos tengan menor relevancia sobre el veredicto final. La compostura será un punto esencial, no debiendo entrar en confrontación con la otra parte, aunque a veces conseguirlo resulte complicado. Y finalmente, si bien en el informe pericial se presenta la necesidad de incorporar una argumentación técnica sólida, en la vista judicial es necesario simplificar al máximo la exposición, de la forma más clara y concisa posible para su entendimiento, sin dejar por ello de respetar la realidad en todo momento.

Otro aspecto clave a tener en consideración es la legitimidad de determinadas prácticas de acceso a la información de los investigados en un caso forense. Es frecuente la duda respecto de la realización de determinadas prácticas de investigación, como puede ser el acceso a las cuentas de correo que proporciona la organización a un usuario y donde residen las evidencias necesarias para el esclarecimiento de un caso. En este tipo de escenarios, la línea que delimita la protección de los datos personales no se encuentra claramente definida. Existen lagunas interpretativas entre la protección en el ámbito estrictamente personal y la que goza la propia empresa para hacer un uso razonable de los medios que proporciona.

5. HIPÓTESIS

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

6. JUSTIFICACION

Que el análisis forense puede ser muy dispendioso y mostrar pocos avances, debido a las características de seguridad con las que se concibe este módulo de investigación.

Sin embargo el análisis facilitara el perito por que posee un conocimiento básico de la estructura de archivos.

6.1 Justificación económica

Es difícil recolectar evidencias debido a los grandes volúmenes de información que actualmente se manejan, la variedad de tecnologías y la dispersión de la misma a lo largo de Internet. Cada día existen mecanismos más sofisticados que permite ocultar y borrar las huellas producto de los delitos informáticos.

6.2 Justificación Social

Se pueden encontrar diversas causas que con llevan a cometer delitos fraudulentos por parte de los funcionarios y empleados en las entidades, entre ellas se tienen:

a) Prácticas contables inadecuadas, que llevan al sometimiento de errores intencionales que distorsionan la presentación de los estados financieros, y que por ende engañan a sus accionistas, inversores, proveedores y hasta instituciones financieras y gubernamentales.

b) Deficiencias en los controles internos de las entidades; se debe entender que un buen sistema de control interno no conlleva a la eliminación de las posibilidades de ocurrencia de irregularidades, sino que éste elimina esas probabilidades. Estas irregularidades como tales se pueden clasificar en tres categorías principales:

i) Perpetradas dentro del sistema de control interno;

ii) Cometidas mediante la manipulación de procedimientos y sistemas del control interno;

iii) Las que se ejecutan por parte de niveles de alto rango jerárquico dentro de la organización.

c) Inadecuada delegación de funciones (En el caso de El Salvador estas normalmente se delegan por confianza).

6.3 Justificación científica

La investigación científica de una escena del crimen es un proceso formal, donde el llamado investigador hace referencia a la participación de diferentes personas, que documentan y adquieren evidencias, usando su conocimiento, técnicas, herramientas y generando indicios suficientes para ayudar a resolver el caso.

7. ALCANCES Y LIMITES

Los pasos para realizar el análisis varían dependiendo del dispositivo o marca de procedencia para luego proceder un análisis minucioso.

7.1. ALCANCES

Sera dar como resultado que en los dispositivos móviles se puedan tener información comparable a la que tiene un computador de escritorio.

7.2. LÍMITES

La cual consiste recuperar todos los archivos de usuario dentro del móvil, a saber: directorio telefónico, SMS, fotos, archivos de sonido, archivos de aplicaciones, etc.

8. APORTES

El aporte será hacer lo referente a la recolección de investigación forense (ver el estado del dispositivo móvil), que existe una gran variedad y dependen del objetivo para la cual van a ser utilizadas.

8.1. PRÁCTICO

Para su desarrollo práctico, cuatro son los pasos a seguir una buena práctica:

a. Preparación y conocimiento general.

b. Recolección y manipulación.

c. Inspección y análisis de la evidencia.

d. Reconstrucción de los hechos.

8.2. TEÓRICO

Teniendo en cuenta el acelerado proceso evolutivo del mundo, en el que se han desarrollado muchos cambios, además del ingreso a la globalización, la seguridad económica resulta ser un factor importante en el desarrollo de cualquier tipo de negocio, en tanto que el ser humano debe afrontar situaciones difíciles que desafían sus principios éticos y valores morales, con actitudes delincuenciales contra el Medio Ambiente.

Como objetivo de este se espera que el asistente, al final de la presentación de la ponencia, pueda comprender la importancia y responsabilidades de la Auditoría Forense Investigativa en el desarrollo de sus labores tanto en el sector público como

privado, y lo trascendental del papel que desempeña el Profesional en cualquier actividad interdisciplinaria, dentro y fuera de las organizaciones económicas y en el desempeño como parte importante en la sociedad y responsabilidad con el Medio Ambiente en la Administración de Justicia, actuando como Perito Auxiliar de la Justicia.

Como competencias en el desarrollo de la presentación los participantes adquirirán interés sobre el saber ser y hacer de la Auditoria Forense en especial cómo se debe aplicar en el Medio Ambiente.

Palabras Claves: Auditoria, Forense, Medio Ambiente, Aplicada al medio ambiente, Fraudes, Delitos.

9. METODOLOGIA

La presente investigación es de tipo descriptivo por sus características así, estas se observaran y se describan tal como se presentan en que cada dispositivo móvil, que posee diversas características en relación a su fabricación y procedencia.

9.1 MÉTODO CIENTÍFICO

Este método científico se suele utilizar para mejora o precisar teorías previas en función de nuevos conocimientos, donde la complejidad del modelo no permite formulaciones lógicas. Por lo tanto, tiene un carácter predominante intuitivo 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 de de servir de marco de generación del conocimiento objetivo, Por ello existen múltiples características en función de la perspectiva con que se clasifican, se estudien e incluso se denominen.

Además los resultados deben ser objetivos e imparciales. La metodología aplicada desde 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, eliminar en la medida de lo posible alternativas plausibles y evitar las conclusiones no falsables. Que una afirmación sea fiable, 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 incluye elementos de la experiencia humana como son las "corazonadas" y la intuición. Estas son de gran utilidad a la hora de proponer hipótesis y modelos que deben ser corroboradas por la fría evidencia, de una forma estricta y objetiva.

CAPITULO II

CAPITULO II

MARCO TEORICO

2.1 INFORMATICA FORENSE

Telefonía Celular GSM en el Bolivia y en el Mundo GSM de las siglas en inglés Global System For Mobile Communications, es un estándar mundial para teléfonos celulares, diseñado para utilizar señales digitales, así como también, canales de voz y canales de control digitales. Existen cuatro versiones principales, basadas en la banda de frecuencia que utilizan para su operación: GSM-850, GSM-900, GSM-1800 y GSM-1900.

En Ecuador la tecnología GSM está siendo utilizada mayoritariamente por las empresas celulares que operan en el país, abarcando con su cobertura a un importante número de usuarios a nivel nacional.

Según la Revista Líderes, Ecuador es uno de los países que más abonados tiene en telefonía móvil a escala mundial. En concreto, posee 12 millones 946 mil usuarios de los 14'306.876 de ecuatorianos. De ellos, 212.842 usuarios tienen contratado el servicio de e-mail para sus teléfonos celulares.

Como muestra la Figura 1, la tecnología GSM es el estándar de telefonía celular más utilizado alrededor del mundo; según GSMA y la Firma de Industrias Móviles Wireless Intelligence, en un reporte de Julio del año 2010, se anunció que el número de conexiones móviles globales ha sobrepasado los 5000 millones en el mercado mundial, después de que a finales del 2008 se registraron 4000 millones de conexiones.

Evidencia Digital

Los elementos de prueba o evidencias dentro de un proceso judicial son de vital importancia, ya que mediante su investigación se puede llegar a determinar la confirmación o desvirtuarían de una hipótesis o afirmación precedente de lo que corresponde a la verdad.

La evidencia digital, es una herramienta de especial cuidado, para el proceso de investigación de delitos tecnológicos; debe ser tratada por parte de especialistas que conserven todas las medidas de precaución necesarias para no contaminarla y/o alterarla, para que ésta no sea objeto de desestimación ante un proceso legal.

Por consiguiente, la evidencia digital no solo está limitada a lo que se encuentra en las computadoras, también se puede extender a los dispositivos electrónicos tales como MP3, memorias flash, Ipod, teléfonos celulares, entre otros aparatos de telecomunicaciones y multimedia.

III. TÉCNICAS DE EXTRACCIÓN DE LA INFORMACIÓN

Evidencia Potencial en la Arquitectura GSM

Dentro de la Arquitectura Instalada Fija de GSM, son de interés como evidencia digital los CDRs (Call Detail Records), que se crean y almacenan en el MSC (Mobile Switching Center) con el propósito de facturación e identificación de las BTS (Base Transceiver Station) sobre las cuales fueron efectuadas llamadas y mensajes de texto, además de información de tiempo y localización del suscriptor.

Este análisis requiere de la participación en su totalidad de la Operadora de Telefonía Móvil, quién muchas veces no está dispuesta a colaborar, por razones de seguridad o cuestiones legales; pero la combinación del análisis de los CDRs con la estación móvil puede ayudar a establecer hechos relacionados con un acto delictivo o puede ayudar a corroborar una coartada.

Evidencia Digital Potencial en el Equipo Móvil

La evidencia digital potencial, es la encontrada en las memorias del Equipo Móvil, ya que muchos fabricantes de teléfonos celulares usan la memoria interna del equipo móvil, para implementar nuevas funciones y almacenar cierta información que no puede ser almacenada en la tarjeta SIM, debido a que tienen especificaciones que permiten el almacenamiento de cierto tipo de información.

En general la evidencia digital lo constituye.

2.2 MARCO REFERENCIAL

El IMEI (International Mobile Equipment Identity)

a) Directorio Telefónico.

b) Historial de Llamadas.

c) Mensajes cortos, Mensajes multimedia, buscadores Web/WAP y correos electrónicos

d) Calendario

e) Otros dispositivos, por ejemplo memorias externas.

f) Evidencia Digital Potencial en la Tarjeta SIM .

El sistema de archivos de la Tarjeta SIM reside en la memoria permanente y está estructurado jerárquicamente. Dispone de tres componentes principales que son: el Archivo Principal (MF) o la raíz del sistema de archivos, los Archivos Dedicados (DF) que sirven como directorios, y los Archivos Elementales (EF) que almacenan los datos.

Dentro de la memoria el espacio es limitado, por tal razón los archivos no son identificados por el nombre, aunque el estándar los asigna, sino por dígitos hexadecimales que tienen una extensión de 2 bytes.

La tarjeta SIM que físicamente constituye evidencia electrónica, almacena información que debe ser discriminada por el examinador o analista forense, con el objeto de encontrar evidencia digital potencial. En la Tabla 1 se muestran los elementos de evidencia digital útil para el examinador forense.

D. Técnicas de Análisis Físico y Lógico para la Extracción de Evidencia Digital de Teléfonos Celulares

Se pueden definir dos técnicas con las cuales se puede extraer evidencia digital de un teléfono celular, la una mediante un análisis físico y la otra empleando un análisis lógico.

El análisis físico implica una copia bit a bit de una entrada física de almacenamiento (chip de memoria); mientras que el análisis lógico implica una copia bit a bit de los objetos lógicos (archivos) que residen sobre un almacenamiento lógico.

2.3.2 CLASIFICACION

Se debe decidir también el orden en el que se va a recoger las evidencias, es recomendable seguir el orden de volatilidad de las mismas. Primero tenemos que asegurar las que puedan ser más volátiles, como puede ser todo aquello que este en la memoria del equipo, cache, estadísticas, etc. Si el dis esta encendido hay mucha información que se perderá en cuanto se apague. Pero también habrá mucha información que se irá corrompiendo con el tiempo que el equipo permanezca

encendido. Esta es la primera de muchas decisiones difíciles que se pueden presentar en el proceso.

A continuación nos encontramos con otro problema fundamental en esta parte del trabajo. Idealmente no deberíamos estudiar la información directamente en su ubicación original. Aunque no siempre es posible o rentable, debemos trabajar sobre copias forenses de la información. Entendemos por copia forense aquella en cuya realización se cumplen dos objetivos fundamentales para la validez del estudio:

1. El origen de la información no ha sido alterado en el proceso de copia o clonación.

2. El resultado es, en los términos que interesan en cada caso, una copia exacta de la evidencia.

Cuanto más sutil sea el rastro a seguir, o mayores hayan sido los esfuerzos por encubrirlo, mas esmero será necesario dedicar en este momento, pues cualquier corrupción de los datos puede dar lugar a que la evidencia se pierda o aparezcan "falsos positivos".

Evidentemente, el destino de la copia debe estar previamente vacio. Y un formateo no es suficiente. En el caso del clonado de una memoria , la mejor forma de asegurarse es que el destino sea una memoria. Y si se trata de un tema delicado, lo mejor es sacarlo de su paquete ante testigos. También puede ser Ml en este momento realizar más de una copia, pues más adelante podríamos no tener esa oportunidad.

2.3.3 DELITOS INFORMATICOS

Durante todo el proceso pericial, no solamente en la fase de recogida de evidencias, hay que llevar un registro completo de todos los pasos que damos. Si además podemos tener testigos, grabaciones, fotos, videos... mejor. No hay nada peor que llegar a la vista y no poder explicar alguna de nuestras conclusiones porque alguno de los pasos que nos llevaron a ella no está documentado. Es importante tomar nota de todo: fechas y horas, personas presentes, como nos encontramos todo, lo que hacemos, porque lo hacemos, cómo y con que lo hacemos.

Para continuar con el laboratorio se hace necesario identificar el tipo de evidencia analizar. Pues aún no se tiene información sobre la misma (bien podría tratarse de una imagen de memoria interna, partición u otro tipo de dispositivo).

Para este propósito bastara, con analizar el funcionamiento del dispositivo móvil haciendo su manejo y funcionamiento del mismo.

Además se debe ver el procedimiento para determinar si el Sistema Operativo del dispositivo móvil tiene todo lo requerido.

El análisis se seguirá mediante un conjunto de herramientas en línea de comandos, desarrolladas solo para dispositivos móviles y que permiten llevar a cabo Análisis el Forenses. Ambas herramientas (TheSleuth Kit y su interfaz web Autopsy) son de libre uso y libre distribución.

Al igual que para las tareas de y existe una distribución favorita conocida como , para las labores relacionadas con la Informática Forense existe otra favorita bajo el nombre de , la cual incluye un completo Set de utilidades que nos facilitan la vida para este tipo de trabajos.

Cabe aclarar que esta no es la única manera de identificar el Sistema Operativo, pues en varias publicaciones se puede ver diferentes métodos de cómo ver lo interno del dispositivo.

El artículo tiene un breve resumen de los detalles, sin embargo se debe considerar otras opciones de clonación, phishing, pharming e incluso manipulación informática en los mismos bancos o en su defecto en los administradores de tarjetas.

Las opciones son varias y se han dado casos en todas partes del mundo. Por otro lado no es suficiente que los bancos se deslinden de la responsabilidad culpando al cliente por no cuidar su tarjeta y su PIN. Vemos que esa es la opción más cómoda tanto para las entidades financieras como para las entidades de regulación. Las medidas son mínimas, las campañas de concientización igualmente. Esperamos que la Ley actué de manera más objetiva.

Para finalizar comentamos una guía de prácticas que pueden resultar útiles para la recolección de evidencias.

El objetivo de esta fase en el ciclo de vida de administración de la evidencia digital es localizar toda la evidencia digital y asegurar que todos los dispositivos móviles sean originales (aquellos disponibles y asegurados en las maquinas o dispositivos) no han sido alterados. Para ello el estándar establece algunos elementos a considerar como:

a) Establecer buenas prácticas y estándares para recolección de evidencia digital

b) Preparar las evidencias para ser utilizadas en la actualidad y en tiempo futuro

c) Mantener y verificar la cadena de custodia

d) Respetar y validar las regulaciones y normativas alrededor de la recolección de la evidencia digital

e) Desarrollar criterios para establecer la relevancia o no de la evidencia recolectada.

Prácticas recomendadas son:

1. Establecer un criterio de recolección de evidencia digital según su volatibilidad:

de la más volátil a la menos volátil.

a) Registros de memoria, memoria cache

b) Tablas de enrutamiento, cache de arp, estadísticas del funcionamiento del sistema operacional.

c) Archivos temporales

d) Almacenamiento en, memorias.

e) Registro remoto de las actividades de la aplicación y monitoreo del trafico de los datos

f) Configuración física de dispositivos y topología de red.

g) Manuales y registros disponibles de los dispositivos y software bajo estudio.

2. Documentar todas las actividades que el profesional a cargo de la recolección ha efectuado durante el proceso de tal manera que se pueda auditar el proceso en si mismo y se cuente con la evidencia de este proceso.

3. Asegurar el área donde ocurrió el siniestro, con el fin de custodiar el área o escena del delito y así fortalecer la cadena de custodia y recolección de la evidencia.

4. Registrar en medio fotográfico o video la escena del posible ilícito, detallando los elementos informáticos alii involucrados.

5. Levantar un mapa o diagrama de conexiones de los elementos informáticos involucrados, los cuales deberán ser parte del reporte del levantamiento de información en la escena del posible ilícito.

2.3.3.1 CASOS DETECTADOS EN BOLIVIA

La Informática Forense ha ingresado en Bolivia en diferentes ámbitos: Académico, profesional, de servicios y empresarial. Podemos ver que es una consecuencia lógica de la batalla entre la seguridad y la inseguridad. Los últimos años vemos un crecimiento marcado de la inversión en seguridad, ¿Pero qué ocurre cuando todo este esfuerzo falla? Tenemos casos como los e-mails de ABC, el hackeo al Sidunea durante el 2007. El 2008 los más notables fueron el phishing al Banco Mercantil que terminó en arrestos en Cochabamba. El fraude de 400 mil Bs. del Banco Bisa. El 2009 hemos comenzado con el fraude a Entel que bordea los 270 mil Bs. y el caso de YPFB donde se están analizando computadores.

Todos estos casos involucran evidencia digital que debe ser tratada bajo estrictos principios de la Informática forense. Vemos un incremento considerable en el uso de recursos tecnológicos para la comisión de delitos tradicionales como narcotráfico, pornografía, homicidios, etc. En las escenas del hecho y durante la investigación es muy frecuente encontrar celulares. Todo esto hace que la Informática forense sea tomada cada día con mayor preocupación.

Los pasos fundamentales al momento de aplicar informática forense son: identificación, adquisición, preservación, análisis y presentación de la evidencia digital. La misma debe cumplir con ciertos requisitos para tener valor probatorio y no quedarse sólo como indicio. Mucho del valor probatorio de la evidencia digital recae en los penta valores de la seguridad: confidencialidad, disponibilidad, autenticidad, integridad y no repudio.

Entre las actividades más destacables en Bolivia, podemos citar el entrenamiento de funcionarios de varias instituciones: Banco Mercantil, Entel, FELCC, FELCN, Vice ministerio anticorrupción, y otros. Entre los pendientes más destacables tenemos la implementación de un laboratorio de Informática forense en el Instituto de Investigaciones Forenses que depende de la Fiscalía General.

A nivel privado Yanapti S.R.L. ya cuenta con el primer Laboratorio forense en Bolivia, con infraestructura, hardware y software especializado de talla mundial.

Entre los eventos realizados durante el 2008 podemos citar las primeras jornadas de Informática Forense con la presencia de 50 efectivos de la Policía Nacional y de 100 profesionales de diferentes empresas. Actividades que contaron con el apoyo de empresas como INFOCRED BIC SA, EDV Bolivia S.A. y la Bolsa Boliviana de Valores.

Otro proyecto importante es el Convenio que se está negociando con diferentes Instituciones para crear las Listas Oficiales de Peritos Informáticos. Se han desarrollado los primeros eventos internacionales en materia de Derecho Informático desde el año 2002. A lo largo de las capitales en Bolivia lleva sus eventos de capacitación donde se combina la seguridad, auditoria de sistemas con el derecho informático y la informática forense.

A la fecha ha desarrollado un programa de capacitación con 180 horas de entrenamiento, teoría y práctica. Que se denomina forensic computer Advisor.

Todos estos antecedentes nos permiten ver que si bien la Informática Forense no es aún lo suficientemente conocida por la población en general, todo este tiempo se ha estado cultivando para solidificar sus cimientos. Ahora consideramos que las bases están sólidas y sobre ellas podemos construir esta rama científica para el apoyo y seguridad de todos.

2.3.4 DELINCUENCIA Y CRIMINALIDAD INFORMATICA

La Informática Forense combina técnicas especializadas con el uso de software sofisticado para ver y analizar información a la que no puede acceder el usuario ordinario. Esta información pudo haber sido "borrada" por el usuario meses o años antes de la investigación o inclusive pudo no haber sido guardada, pero puede aún estar presente en todo o en parte, en el disco duro de la computadora.

Es siempre recomendable para precautelar el interés del abogado, del cliente y de otros aspectos legales que se está tratando, el encontrar a un especialista que nos asista en todas las etapas, en la preparación de un proceso judicial, incluyendo aspectos como:

- Determinar si la computadora en cuestión tiene o no información relevante al proceso judicial.

Para determinar si la computadora contiene información que puede servir como prueba o evidencia, el profesional debe, primero, crear una copia del disco duro en cuestión, "imagen exacta del disco duro". El experto sólo examinará esta copia, protegiendo así el disco original de alteraciones inadvertidas. Esta imagen debe ser real BIT a BIT o milímetro a milímetro del original, no una simple copia de la información del original, sino una copia completa. Adquirir estas copias exactas, requiere el uso de técnicas forenses especializadas.

Estas copias "imagen exacta" son muy importantes, ya que cada vez que alguien enciende una computadora, muchos cambios son automáticamente hechos en la mayoría de los archivos. Por ejemplo, en un sistema Windows convencional, más de 160 alteraciones son hechas a los archivos, cuando una computadora es encendida. Estos cambios no son visibles para el usuario, pero estos cambios, que sí ocurren, pueden alterar o inclusive borrar evidencia, por ejemplo: fechas importantes relacionadas con la actividad criminal.

Asegurar la cadena de la prueba (que se refiere básicamente al momento desde la sospecha del abogado o de la parte, de que alguna información que puede ser usada como evidencia, está en una computadora, el primer acercamiento y evaluación del experto hasta el informe final) es tan importante para el especialista que hace la primera evaluación del disco y la evaluación de la información por su valor como evidencia, así como lo es para un médico forense en su área. El especialista en Informática Forense usa los denominados HASH CODES o Códigos Aleatorios para asegurar la cadena de custodia. Estos son cifras numéricas realmente largas, específicas para cada archivo y para cada disco, que son calculadas matemáticamente.

Si un archivo o disco es cambiado inclusive en su más mínima parte, este Código Aleatorio también cambiará.

i) Asistir en la preparación y respuesta a interrogatorios.
ii) Recibir y examinar información que está sólo accesible a través del uso de métodos y programas forenses.

El análisis de informática forense es siempre útil en aspectos que aparentemente parecen poco relacionados con las computadoras. En algunos casos, información personal en una computadora, por ejemplo, en un caso de divorcio, el esposo puede haber escondido fondos mancomunados en una cuenta de banco secreta. En otro caso, un empleado, para comenzar su propia empresa, puede haber renombrado un paquete de computación desarrollado por su actual empleador. A pesar de que todos los actores en los casos mencionados han borrado la información que tienen en sus computadoras, el especialista en Informática Forense puede recuperar esta información de los discos duros de las computadoras.

iii) Planificar y proveer testimonio del perito.

Elementos a recuperar.-

a) Recolección de evidencias en su almacenamiento y administración de aplicaciones
b) Recuperación de contraseñas
c) Detección y recuperación de datos
d) Seguridad en el correo electrónico
e) Análisis de Redes GSM7 WCDMA Y WCDMA
f) Procesos en el puesto de usuario
g) Anonimato
h) Investigación de información

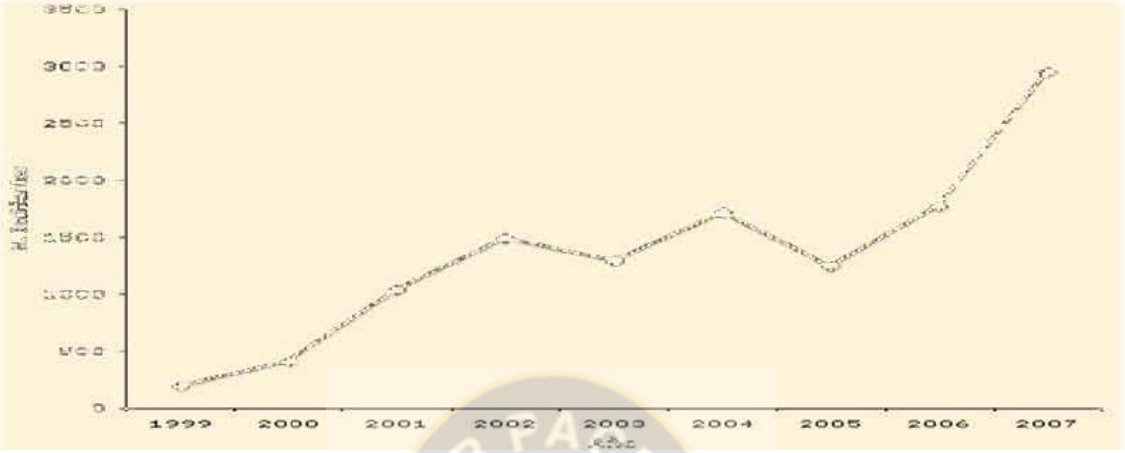


Figura : 1.2 Evolución de incidentes de seguridad

Fuente : rediris-Informe de Evolución de Seguridad 2007

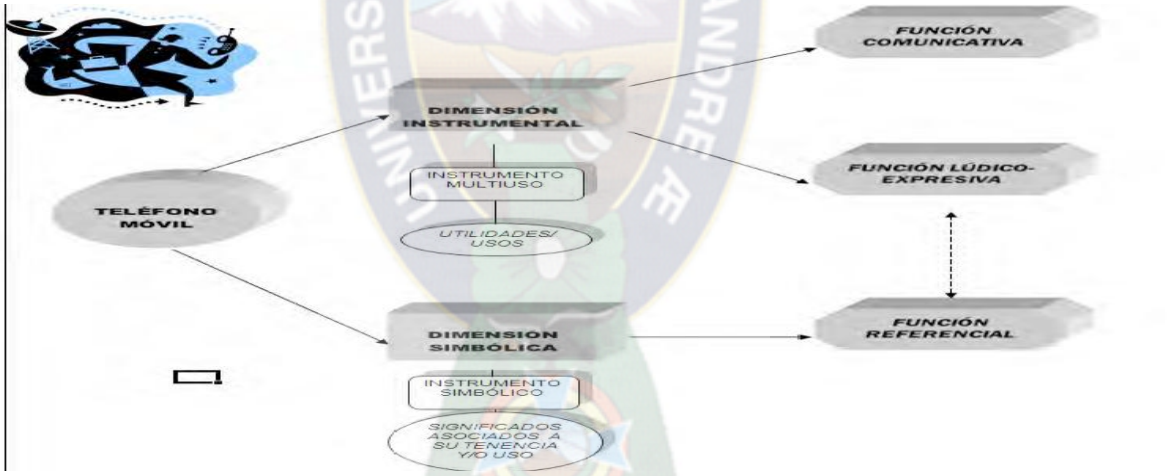


Figura 2.2 : CASOS REGISTRADOS EN BOLIVIA SOBRE DIMENSIONES Y FUNCIONES DEL TELÉFONO MÓVIL.

Fuente : FELCC

2.3.5 EVIDENCIA DIGITAL

La evidencia digital es frágil y volátil. La información residente en los medios de almacenamiento electrónico puede ser borrada, cambiada o eliminada sin dejar rastro, lo cual limitara labor del investigador forense en informática tendiente a identificar y encontrar elementos clave para esclarecer los hechos relevantes de una investigación.

En este sentido, las pruebas digitales son piezas probatorias básicas que requieren una revisión detallada sobre cómo se crean, recolectan, aseguran y, finalmente, cómo se presentan en la corte a efecto de aportar, con claridad y precisión, factores que orienten las decisiones en casos donde sean parte fundamental.

Al ser un objeto relativamente fácil de manipular, generado por dispositivos electrónicos de los cuales no sabemos nada sobre su funcionamiento, la susceptibilidad a las fallas, entre otras características, nos advierte que estamos entrando en un campo de investigación delicado y formal donde el conocimiento técnico están fundamental como el forense y el de técnicas probatorias.

En razón de lo anterior, es preciso indagar sobre estrategias para implantar reglas mínimas que le permitan a la corte validar o no pruebas digitales. Si bien esta labor requiere un entendimiento técnico de los medios electrónicos, también establece un reto a los fiscales y jueces para involucrarse en los cambios que establece una sociedad digital, donde la delincuencia también ha evolucionado en sus métodos y estrategias delictivas.

Al aportar elementos digitales en un caso, es preciso que el aparato judicial tenga una base formal y clara sobre la admisibilidad de la ED presentada, es decir, que la administración de justicia pueda contar con características básicas de las pruebas e implementar procedimientos básicos con los que pueda verificar su autenticidad, confiabilidad, suficiencia y conformidad con las leyes establecidas.

Este documento tratará de revisar una serie de características técnicas y conceptos legales que permitan establecer una relación viable entre ambos mundos, para desarrollar elementos de admisibilidad de evidencia digital como un punto de inicio en la discusión de un tema que plantea retos tanto para la tecnología informática y sus medios de protección como para la justicia en el entendimiento y seguimiento de los delitos informáticos.

2.3.5.1 CARACTERISTICAS DE LA EVIDENCIA DIGITAL

La evidencia digital posee las siguientes características:

i. Volátil
ii. Anónima
iii. Duplicable
iv. Alterable y modificable
v. Eliminable

Estas características hacen de la videncia 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 tecnologías para obtener, custodiar, revisar, analizar y presentar la evidencia en una escena del delito. Antes de realizar el proceso de auditoría forense el equipo de seguridad o auditoria debe considerar los siguientes elementos para mantener la idoneidad del procedimiento forense.

a) Evidencia altamente volátil

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

b) 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.

c) 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 registros 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].

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 corresponden a la realidad evidenciada en la fase 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 ismos en las organizaciones , mientras que para los registros magnéticos aun no se tiene misma formalidad.

Verificar la autencidad de los registros digitales requiere, de manera complementaria, a la directriz general establecida por la organización sobre estos, el desarrollo y configuración de mecanismos de control de integridad de archivos, es decir. Necesaria 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 registros y el procedimiento asociado para su verificación, aumentando 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 solo por lo que su contenido ofrezca, sino por las condiciones de generación, control y revisión de los registros electrónicos.

En otras palabras, el 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 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 que poseen una manera confiable para ser identificados, recopilados y verificados.

Cuando logramos que una arquitectura de computo 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 programa es necesario incluir, desde las primeras fases de la creación de aplicaciones, un momento para la configuración de logs o registros de auditoria del sistema ya que , de no hacerlo, se corre el riesgo de perder trazabilidad 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 computo estará en función de la manera como se sincronice la inscripción de las acciones de los usuarios y de un registro centralizado e integro 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 procesos

Que podrían haberse resultado. 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 esta particularidad 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.

---

1 Trazabilidad – Capacidad de seguimiento y reconstrucción de acciones efectuados por lo usuarios en un sistema

Si analizamos esta posibilidad, es viable establecer relaciones entre los datos 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 este en mente, la correlación se convierte en factor aglutinante de las características anteriores referenciadas para integridad y confiablidad 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 computo para asegurar la suficiencia del análisis de la información presente en una arquitectura de computo.

2.3.6.4 CONFORMIDAD CON LAS LEYES Y REGLAS DE LA ADMINISTRACION DE JUSTICIA

Hace referencia a los procedimientos internacionales aceptados para recoeccion, aseguramiento, análisis y reporte de la evidencia digital. Si bien están previstos en el código de procedimiento penal las actividades mínimas requeridas para optar evidencia a los procesos, existen en medios digitales iniciativas internacionales donde se establecen lineamientos de acción y para metros 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 el registro electrónico que tenga signo distintivo de autoría, autenticidad y que sea fruto de la correcta operación confiabilidad del sistema.

b) Regla 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 LEGISLACION BOLIVIANA

Art. 1º.- El Estado boliviano a través del Poder Legislativo, Ejecutivo, Judicial, Prefecturas de Departamento, Gobiernos municipales, entidades descentralizadas, desconcentradas y otras donde el estado tenga participación, emplearan prioritariamente el Software libre desarrollado con estándares abiertos en sus sistemas, proyectos y servicios informáticos. Para este fin las entidades estatales de la administración pública deben iniciar el proceso de migración gradual y progresiva hacia el software libre.

Art. 2º.- Todas las entidades estatales deberán dar uso o contratación de licencias de software libre frente a licencias que tengan privacidad en su uso.

Art. 3º.- Las entidades educativas estatales, privadas, descentralizadas y de convenios, donde tenga participación el Estado, deberán incluir en su curricular programática de sus educandos la utilización del software libre.

Art. 4.- El Estado deberá intercambiar la información a través de Internet en al menos un navegador de Internet basado en Software Libre.

Art. 5.- El estado debe fomentar el desarrollo de la industria de SW libre (con estándares abiertos) promoviendo la investigación en ciencia y tecnología en todos sus niveles, con incentivos para los desarrolladores.

Art. 6.- El estado boliviano a través del Poder Ejecutivo deberá desarrollar una versión propia de un sistema operativo basado en software libre.

Art. 7º.- El poder ejecutivo reglamentará en un plazo de 90 días las condiciones y formas de migración de la situación actual, a la adecuación de la presente Ley, en todas las entidades contempladas en los Art. 1º y 3º de la presente Ley.

La Informática Forense ha ingresado en Bolivia en diferentes ámbitos: Académico, profesional, de servicios y empresarial. Podemos ver que es una consecuencia lógica de la batalla entre la seguridad y la inseguridad. Los últimos años vemos un crecimiento marcado de la inversión en seguridad, ¿Pero qué ocurre cuando todo este esfuerzo falla? Tenemos casos como los e-mails de ABC, el hackeo al Sidunea durante el 2007. El 2008 los más notables fueron el phishing al Banco Mercantil que terminó en arrestos en Cochabamba. El fraude de 400 mil Bs. del Banco

Bisa. El 2009 hemos comenzado con el fraude a Entel que bordea los 270 mil Bs. y el caso de YPFB donde se están analizando computadores.

Todos estos casos involucran evidencia digital que debe ser tratada bajo estrictos principios de la Informática forense. Vemos un incremento considerable en el uso de recursos tecnológicos para la comisión de delitos tradicionales como narcotráfico, pornografía, homicidios, etc. En las escenas del hecho y durante la investigación es muy frecuente encontrar celulares. Todo esto hace que la Informática forense sea tomada cada día con mayor preocupación.

Los pasos fundamentales al momento de aplicar informática forense son: identificación, adquisición, preservación, análisis y presentación de la evidencia digital. La misma debe cumplir con ciertos requisitos para tener valor probatorio y no quedarse sólo como indicio. Mucho del valor probatorio de la evidencia digital recae en los penta-valores de la seguridad: confidencialidad, disponibilidad, autenticidad, integridad y no repudio.

Entre las actividades más destacables en Bolivia, podemos citar el entrenamiento de funcionarios de varias instituciones: Banco Mercantil, Entel, FELCC, FELCN, Vice ministerio anticorrupción, y otros. Entre los pendientes más destacables tenemos la implementación de un laboratorio de Informática forense en el Instituto de Investigaciones Forenses que depende de la Fiscalía General.

A nivel privado Yanapti S.R.L. ya cuenta con el primer Laboratorio forense en Bolivia, con infraestructura, hardware y software especializado de talla mundial.

Entre los eventos realizados durante el 2008 podemos citar las primeras jornadas de Informática Forense con la presencia de 50 efectivos de la Policía Nacional y de 100 profesionales de diferentes empresas. Actividades que contaron con el apoyo de empresas como INFOCRED BIC SA, EDV Bolivia S.A. y la Bolsa Boliviana de Valores.

Otro proyecto importante es el Convenio que se está negociando con diferentes Instituciones para crear las Listas Oficiales de Peritos Informáticos. Se han desarrollado los primeros eventos internacionales en materia de Derecho Informático desde el año 2002. A lo largo de las capitales en Bolivia lleva sus eventos de capacitación donde se combina la seguridad, auditoria de sistemas con el derecho informático y la informática forense.

A la fecha ha desarrollado un programa de capacitación con 180 horas de entrenamiento, teoría y práctica. Que se denomina forensic computer Advisor.

Todos estos antecedentes nos permiten ver que si bien la InformáticaForense no es aún lo suficientemente conocida por la población en general, todo este tiempo se ha estado cultivando para solidificar sus cimientos. Ahora consideramos que las bases están sólidas y sobre ellas podemos construir esta rama científica para el apoyo y seguridad de todos.

Delitos Informáticos

Articulo 363.- Bis (manipulación informática). El que con la intención de obtener un beneficio indebido para sí o un tercero. Manipule un procedimiento o transferencia de datos informáticas que conduzca a un resultado incorrecto o evite un proceso tal cuyo resulta 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.

Articulo363.- Ter (Alteración acceso y uso indebido de datos informática). El que sin estar autorizado apoderare, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicios al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.[CódigoPenal, 1999].

2.5 MARCO TECNOLOGICO

2.5.1 HERRAMIENTAS FORENSES

El uso de las herramientas en Bolivia se basan procesos, donde la Informática Forense puede ser usada para descubrir evidencia potencial en una variedad de casos, incluyendo:

a) Delitos contra la Propiedad Intelectual, en caso de Software Pirata o documentos con el debido registro de derechos de Autor. LEY No. 1322 DE 13 DE ABRIL DE 1992.
b) Robo de Propiedad Intelectual y Espionaje industrial (que aunque no se crea, sí existe en nuestro país).
c) Lavado de Dinero, vía transferencia de fondos por Internet.
d) Acoso Sexual (vía e-mail); Chantaje o amenazas (vía e-mail).

e) Acceso no autorizado a propiedad intelectual.
f) Corrupción.
g) Destrucción de Información Confidencial.
h) Fraude (en apuestas, compras, etc. Vía e-mail).
i) Pornografía en todas sus formas, inclusive en la más devastadora: Pornografía infantil.

Ejemplos de artículos relacionados con Forensic.-

i) Herramienta forense comercial puede quebrar el cifrado de Bitlocker
ii) Hackers le declaran la guerra a una herramienta forense internacional

2.5.2 CONFIABILIDAD 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 forense 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 los especialistas forenses deben constantemente reforzar sus habilidades en el uso de estos programas y mantenerse notificaciones de posibles errores, propios de las mismas y sus maneras de mitigarlos pues que un caso basado en la confiabilidad de las mismas se puede o no decidir.

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 uso pruebas, de las cuales personas 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 eta 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 mejorar.

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 tenías sobre su uso del teléfono móvil, pero sobre todo se hará conocer si el equipo es original y si especifica todas las funciones que tiene ,pero sino rinde las condiciones se hará la recolección de la información y dar una posible impunidad, o ser anuladas o inadmisibles y llevar a un juicio basadas con las leyes que rige en nuestro país.

Esa evidencia 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 o de la empresa encargada que hace su distribución, sin sufrir las consecuencias de la nulidad de las pruebas o la inadmisibilidad de estas en el juicio.

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

Tabla: 2.3 Método de Análisis Forense

Fuente: [Elaboración Propia]

3.1 FASE DE IDENTIFICACION

En esta primera fase se debe asegurar la integridad de la evidencia en los dispositivos móviles , es decir, que no se deben realizar modificaciones ni alteraciones sobre dicha evidencia, en este aspecto tratar de mantener los requerimientos legales.

De un tiempo acá, los productos de Apple han causado una verdadera revolución en cada mercado donde han entrado, la música, la telefonía móvil y ahora con la salida de su tableta iPad se ha creado un nuevo mercado que augura la era post-pc y ha cambiado la forma de consumir contenidos.

Todos estos dispositivos móviles de Apple *(iPhone, iPad, iPod Touch, Apple TV, etc…)* tienen como sistema operativo una variante de Mac OS X *(específicamente de su kernel)* adaptada para tal fin, con nombre iOS y es precisamente sobre el análisis forense a este sistema operativo que hablaremos en esta serie de artículos.

El análisis forense de dispositivos iOS es un área poco explorada en nuestro idioma, existen algunos algunos textos de referencia en ingles, y productos comerciales para llevar a cabo esta tarea, pero poca o nula información sobre los procedimientos, técnicas y metodologías a tener en cuenta a la hora de realizar un análisis forense a estos dispositivos móviles de Apple en español.

Es por esto que lanzamos esta serie de artículos titulados "Análisis Forense de Dispositivos iOS" para contribuir un poco con documentación en nuestro idioma sobre estos procesos forenses y complementar la información de mi futura charla en la EKO Party 2011 sobre este tema.

El análisis forense de dispositivos iOS inicia como cualquier otro análisis forense, solo debemos tener en cuenta que algunos de estos dispositivos con iOS son teléfonos móviles, por tanto debemos tener las precauciones necesarias para estos dispositivos en especial y nos guiaremos por el siguiente diagrama que he traducido para este articulo.

Adicionalmente, es preciso que el investigador o especialista se cuestione sobre la información obtenida en un sistema de información que sea está comprometido. en la cual se pregunta.

a) ¿Qué información se necesita?

b) ¿Cómo aprovechar la información presentada?
c) ¿En qué orden ubico la información?
d) ¿Acciones necesarias a seguir para el método de análisis forense en el dispositivo móvil?

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

Lo que se debe realizar en esta fase es la evaluación de los recursos a los que tenemos acceso y cuáles son los objetivos para realizar la investigaron interna, pasando por las siguientes etapas:

. Notificar y obtener la autorización: En esta etapa del proceso forense, debemos obtener una autorización por escrito para iniciar el análisis forense , al igual que la firma de los acuerdos de confiabilidad, sin esta autorización por escrito nuestro análisis no tendría una validez legal y de hecho estaríamos cometiendo un delito.

. Revisar las políticas y la legislación: Debemos documentos sobre todas las políticas y legislación vigente para el análisis forense y manejo de evidencias en el país donde se presente el incidente, además de todas las acciones y antecedentes que proceden la investigación.

. Realizar una evaluación: Debemos realizar una investigación preliminar que nos permita exponer la situación actual , hechos sucedidos, las personas u organizaciones afectadas, posibles sospechosos, gravedad y criticidad de la situación, daños causados(clientes, impacto financiero, I+D, etc.,..), identificar topología(red, equipos, SO, etc.,..) , realizar entrevista con funcionarios, usuarios administradores y responsables de los sistemas , con esto lograremos tener un panorama mas claro que nos facilite una mejor comprensión de la situación.

Al terminar esta etapa del análisis del dispositivo móvil debemos entregar un documento con toda la información detallada de los procedimientos realizados, para establecer el inicio de la adquisición de datos, la cadena de custodia y la elaboración de los informes finales.

La solicitud forense es un documento donde el administrador del dispositivo móvil 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:

DESCRIPCION DEL DELITO INFORMATICO

a) Fecha del incidente
b) Duración del incidente
c) Detalles del incidente

INFORMACION GENERAL

a) Área
b) Nombre de la dependencia
c) Responsable del área del dispositivo afectado
   i) Nombres y apellidos
   ii) Cargo
   iii) E-mail
   iv) Teléfono
   v) Extensión
   vi) Celular
   vii) Fax

INFORMACION SOBRE EL DISPOSITIVO MOVIL (AFECTADO)

a) Nombre del equipo
b) Marca y modelo
c) Capacidad de la memoria interna
d) Capacidad de la memoria externa
e) Modelo
f) Sistema operativo (nombre y versión)
g) Función del equipo
h) Tipo de información procesada por el equipo

Toda la información del incidente, la evidencia digital, copias o imágenes de la escena del crimen, se basa en una tabla que se ve a continuación.

METODO ANALISIS INFORMATICO FORENSE

1. DESCRIPCION DEL DELITO INFORMATICO

Fecha del incidente: _____

Si se puede establecer, ¿Cuál fue la duración del incidente? _____
En pocas palabras, enumerare los detalles del incidente
¿Cómo se descubrió?

_____

_____

Si es posible realizar un diagnostico, brevemente describir el método utilizando para obtener acceso al dispositivo móvil y que vulnerabilidades fueron aprovechadas (clave fácil, deficiencia en los controles, etc.).

_____

_____

Describa las medidas que fueron tornadas para atender el incidente:

iii) Ninguna en especial
iv) Reinstalación del sistema
v) Aplicaciones en funcionamiento
vi) Recuperación de copias de seguridad
vii) Cambio de equipo
viii) 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. INFORMACION GENERAL

Área: _____

Nombre de la empresa móvil: _____

TABLA DE SEGUIMIENTO

Responsable de la venta de dispositivos móviles (Persona con quien está encargadode la distribución de dichos equipos y la cual se puede comunicarse y que conoce los detalles del incidente)

Nombre y apellidos: _____

Cargo: _____

E-mail:_____ **Telf.:**_____

Extensión: _____ **Celular:** _____ **Fax:** _____

Si sabe de otro equipo(s)que haya sufrido el mismo problema o uno similar, diga cual (es).

_____

_____

3. INFORMACION SOBRE EL EQUIPO AFECTADO

(Información sobre, sistema operativo y red. Si hay más sistemas, llene otro formato)

Dirección IMEI : _____ **Nombre del equipo:** _____

Marca y Modelo: _____

Capacidad de la Memoria interna _____**Capacidad en memoria externa** _____

Modelo del teléf. móvil: _____

Sistema Operativo (nombre y version): _____

Funcion del Dispositivo Movil:_____

_____

Tipo de informacion procesada por el equipo: _____

_____

Acto realizado por el Fiscal: _____

Con la intervencion de los investigadores: _____

Peritos informaticos Forenses: _____

_____

En presencia del testigo: _____

Con CI : _____ **RUN:**_____ **PASAPORTE N°:**_____

Observaciones:

_____

_____

Con lo que termino el acto a horas…….. Del día ….. Del mes……..año……..
Firmando al pie los intervinientes:

Fiscal:……..

Investigar Asignado al caso:…….

Investigar Especial:……

Perito Informático Forense (1):…….

Perito Informático Forense (2):…….
Propietario:…….

Ocupante:……

Testigo:……

Otros:……..

Figura 3.3: 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 la recolección de las evidencias debe estar capacitado y entender a fondo el método.

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

b) Si al momento de dar funcionamiento al equipo móvil , y alguien se encuentra operando otras maniobras falsas al equipo móvil para dar convencimiento de su procedencia ,pero por dicha manipulación se procederá a ser involucrado en el posible ilícito, tomar nota de la situación y fotografiarlo cuando aún está sentado en posición de operador.

c) Pedir a la persona que se encuentra encargada de la venta de móviles que suspenda de manera inmediata lo que está haciendo.

d) 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 disquetes),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 atodos los procesos necesarios para la presentación de resultados finales. La evidencia se clasifica según:

3.1.1.3 PRIORIDAD DEL ADMINISTRADOR

Las evidencias se pueden clasificar según la prioridad del administrador, las mismas están basadas en 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 aplicado la siguiente fórmula

CRITICIDAD DE LOS DAÑOS= EXTENSION DE DAÑOS PRODUCIDOS+ CRITICIDAD DE LOS RECURSOS AFECTADOS

La extensión de los daños producidos es:

a) **Graves.-** Que el incide produjo daños muy severos sobre los servicios o información.
b) **Moderados.-** Que el incidente causo molestias y perdida de información.
c) **Leves.-** Que el incidente producido no tiene mayor importancia, pero si una la mala distribución de los equipos móviles.

La criticidad de los recursos afectados es:

a) **Alta.-**Los recursos afectados son muy importantes dentro de la sociedad y como tal comprometen el normal funcionamiento y prestación de servicios.
b) **Media.-** Los recursos afectados causan molestias al área del comercio y distribución de estos equipos según procedencia.
c) **Baja.-** Los recursos afectados causan ciertas molestias pero se puede seguir con el normal funcionamiento de los equipos.

Un claro ejemplo podemos ver en la siguiente imagen del funcionamiento de la criticidad y sus efectos:

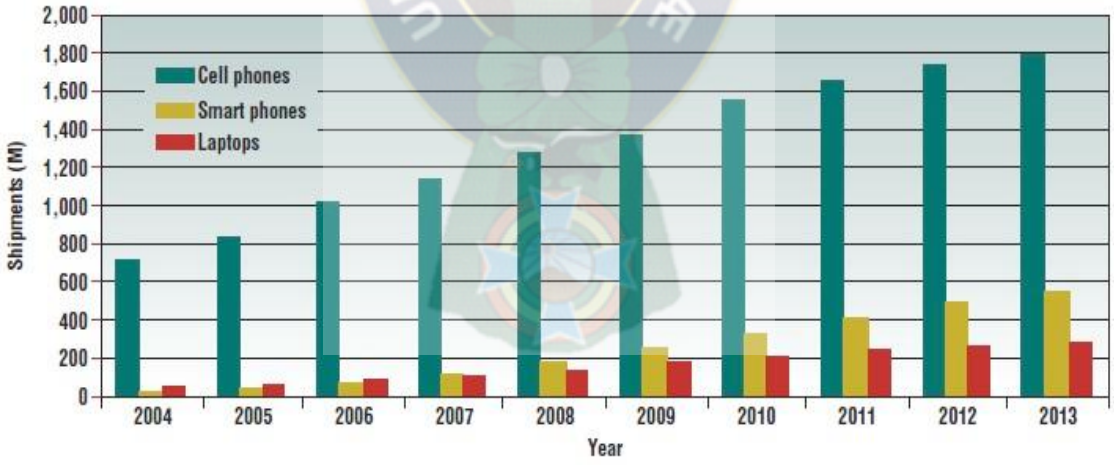
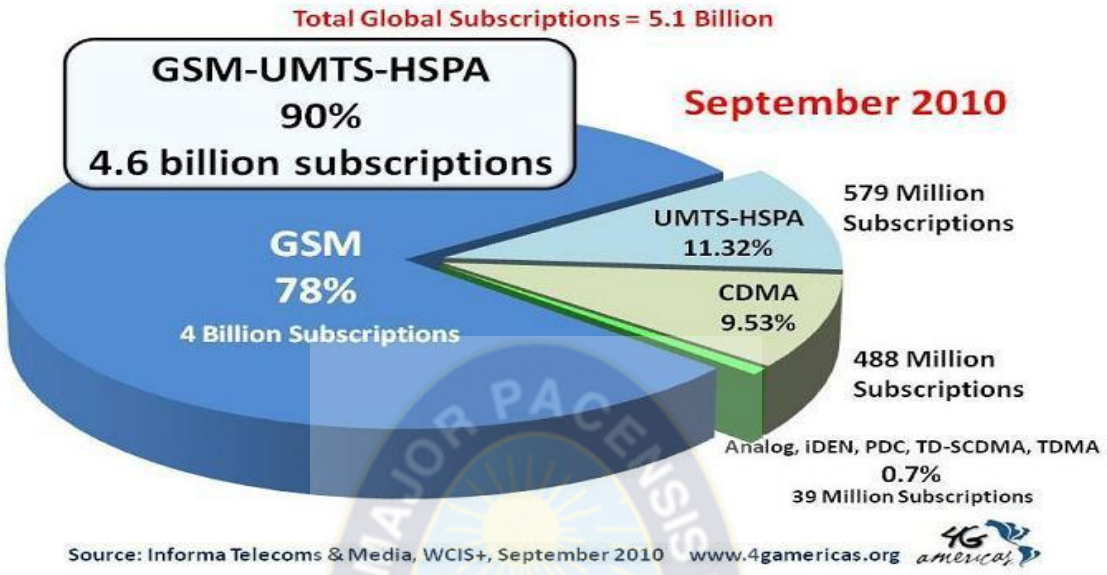


Figura 2.3. Evolución de los pedidos de móviles, terminales inteligentes y portátiles



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:

a) Sistemas informáticos
b) Redes Inalámbricas
c) Dispositivos móviles
d) Sistemas embebidos
e) Otros dispositivos

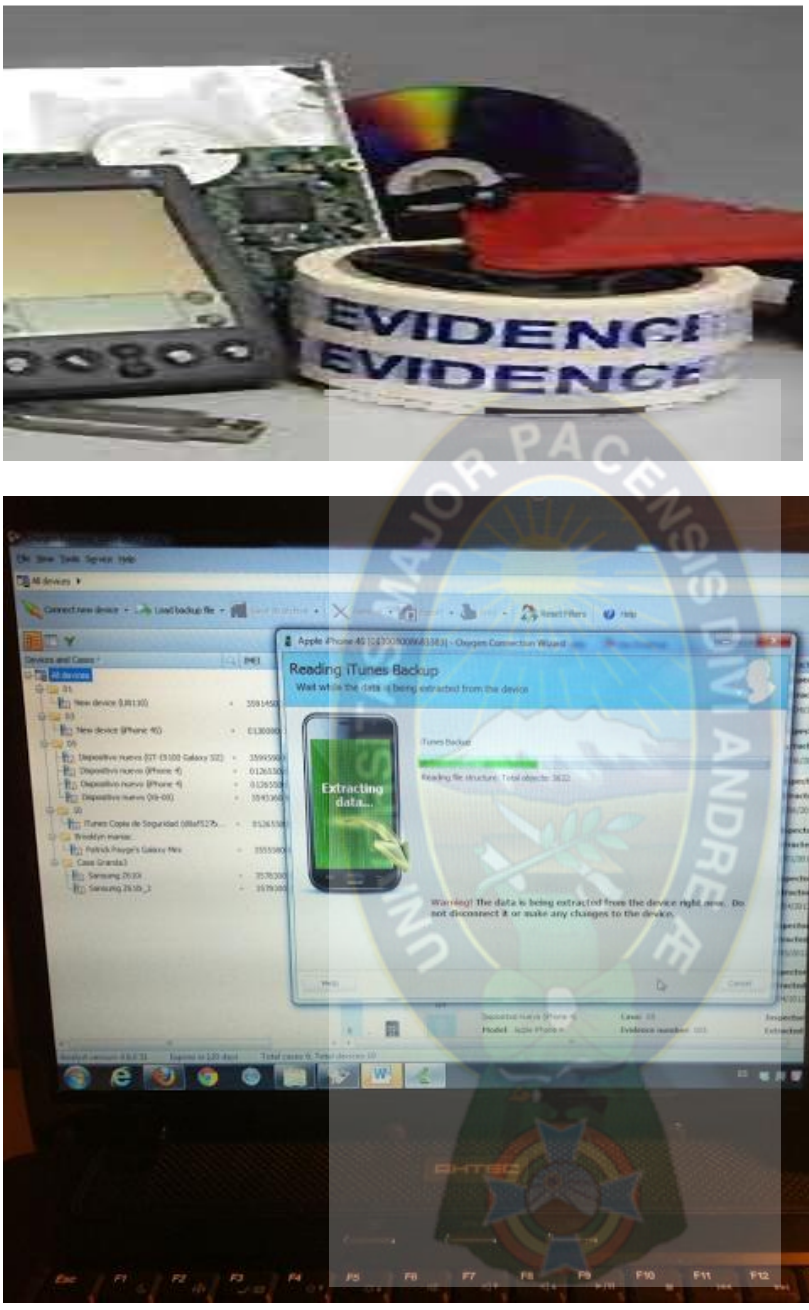


Figura 2.4 : Análisis Forense a un iPhone 4S con iOS6 usando Oxygen Forensics

3.1.1.5 MODELO DE ALMACENAMIENTO

A las evidencias también se las clasifica según el medio de almacenamiento,

Como pueden ser:

I)**Volátiles.-** Aquellas que se perderán al apagar el equipo como la otra 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.

ii)**No volátiles.-** Medios físicos de almacenamiento como memorias flash, CD, discos duros.

6 Sistemas embebidos la denominación de Sistemas (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.

a) Identificar los dispositivos informáticos que almacenen grandes volúmenes de información digital (computadora de escritorio, computadora portátil y discos duros portátiles.
b) Identificar memorias, interna y salida relevantes a la investigación.
c) Identificar si existe periféricos conectados a los equipos informáticos., realizar fotografías de las mismas.
d) Identificar el posible delito que se hubiese cometido en la escena del hecho, determinar los presuntos actores involucrados, maquinas y/o usuarios y la posible participación que tuvo cada uno.
e) Realizar entrevistas al personal de la organización que tenga algún tipo de relación con el entorno informático.
f) 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 si mismos, los siguientes comprobantes de posible existencia:

i) Comprobantes de pago/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.
ii) Anotaciones de claves de usuario o de correos que pudieran encontrarse en soportes distintos a los electrónicos (papeles)
iii) Comprobantes de operaciones realizadas con tarjetas de crédito o débito.
iv) Comprobantes emitidos por cajeros automáticos.
v) Listados de estados de cuentas bancarias.
vi) Plásticos o tarjetas de crédito o débito.
vii) Plásticos de tarjetas de hoteles u otras con banda magnética.
viii) 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 método análisis forense comprende la identificación, y búsqueda de evidencias. Se debe identificar qué cosas pueden ser evidencias, donde y como esta almacenada, que 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 aplicaciones a utilizar.

3.2 FASE DE RECOLECCION

Dentro de la Arquitectura Instalada Fija de GSM, son de interés como evidencia digital los CDRs (Call Detail Records), que se crean y almacenan en el MSC (Mobile Switching Center) con el propósito de facturación e identificación de las BTS (Base Transceiver Station) sobre las cuales fueron efectuadas llamadas y mensajes de texto, además de información de tiempo y localización del suscriptor.
Este análisis requiere de la participación en su totalidad de la Operadora de Telefonía Móvil, quién muchas veces no está dispuesta a colaborar, por razones de seguridad o cuestiones legales; pero la combinación del análisis de los CDRs con la estación móvil puede ayudar a establecer hechos relacionados con un acto delictivo o puede ayudar a corroborar una coartada.

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.

A) 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 aun se encuentren en la "escena del delito" e incluso puede resultar en el impedimento de llevar a cabo las acciones legales pertinentes.

B) En el caso de que se elija la segunda alternativa y el profesional se encuentra capacitado para realzarlo, 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 recolección:

a) Utilizar pulseras antiestáticas para evitar daños en los componentes electrónicos dentro del dispositivo móvil y aguantes de látex para no alterar, encubrir o hacer desaparecer las huellas dactilares existentes en el equipo.

b) 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).

c) Proceder con el acordonamiento del lugar y asegurar el área donde ocurrió el incidente, con el fin de custodiar la escena del derecho y así fortalecer la cadena de custodia y recopilación de la evidencia.

d) Según el RFC 3227 , la evidencia debe ser recolectada de lo más a lo menos volátil. A continuación se presenta una posible clasificación según el orden de volatilidad:

i) Evidencia altamente volátil

Equipo móvil (Registros, Cache), memoria ,cámara 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 equipo movil.

ii) Evidencia medianamente volátil

La memoria, incluye el campo de información a guardarsesobre los procesos en ejecución y requiere conocimiento especializado para su buen manejo y utilidad,

iii) Evidencia poco volátil
iv)

Medios fijos (red inalámbrica y acceso a internet), de esta la información recolectada en el área permitirá analizar los procesos y la información de los mismos en un punto del tiempo en particular. Los directorios permiten reconstruir eventos.

Las evidencias que se recolectan 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 investigación, bajo constancia en acta, con la firma de todos los participantes y un testigo de actuación.

3.3 FASE PRESERVACION

Aunque el primer motivo de la recolección 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 como ha sido preservada la evidencia tras la recolección de la evidencia.

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

Se pueden definir dos técnicas con las cuales se puede extraer evidencia digital de un teléfono celular, la una mediante un análisis físico y la otra empleando un análisis lógico.

El análisis físico implica una copia bit a bit de una entrada física de almacenamiento (chip de memoria); mientras que el análisis lógico implica una copia bit a bit de los objetos lógicos.

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 una.

Para la extracción de información del teléfono celular, se debe considerar que este tipo de información se encuentra retenida o almacenada en las memorias internas

del mismo, además se puede encontrar información valiosa en la tarjeta SIM. Para analizar esta información se consideran los niveles de extracción.

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:

i) Donde, cuanto y quien examino la evidencia, incluyendo su nombre, su cargo, un numero identificativo, fechas y horas , etc.
ii) Quien estuvo custodiando la evidencia, durante cuánto tiempo y donde se almaceno.
iii) Cuando se cambie la custodia de la evidencia también se deberá documentar cuando y como se produjo la transferencia y quien la transporto.

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 permitirá investigar las causas y posibles responsables.

La cadena de custodia deberá contener información sobre el dispositivo incautado, numero 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.

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 videncia:

_____

Nombre posición e institución de quien hizo la recolección de la evidencia:

_____

Datos de evidencia:

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

Tipo: _____

Descripción: _____

Características físicas: _____ **Números Seriale** _____

Nº	Entrega 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 4.3: Acta para la identificación y cadena de custodia

Fuente: Elaboración propia

3.4 FASE DE ANALISIS

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 re colecc ionadas y almacenadas de forma adecuada, iniciamos la fase más laboriosa, el Análisis Forense propiamente dicho, cuyo objetivo es reconstruir con todos datos disponibles, determinando la cadena de acontecimientos que tuvieron lugar desde el inicio de la compra, hasta el momento de su descubrimiento.

3.4.1.1 PASOS PARA REALIZAR UN METODO DE ANALISIS 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 reconstituyen la información inicial. Estos elementos son:

Descripción de los pasos:

1. **Creación del archivo de hallazgos**

   Consiste en la creación y el aseguramiento de un documento, ya sea físico 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 haya sido analizado.

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**

   Para 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 proveído en el caso.

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 un acopia.

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 tengo ningún tipo de virus conocido.

   Luego se debe verificar la integridad de la copia, de la misma forma como se hizo con la original. 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 las estrategias de recuperación de archivos adecuada.

8. **Identificación del sistema de los programas en el equipo móvil**

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

9. **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, pueden no ser posible la recuperación de la totalidad de los archivos eliminados por ejemplo, si estos han sido sobre escritos, o si sean utilizado herramientas de borrado seguro para eliminarlos

   Los archivos recuperados exitosamente formaran 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.

10. **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 los archivos protegidos también se tendrán en cuenta durante la etapa de análisis de este tipo de archivos.

11. **Identificación de archivos existentes**

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

12. **Identificación de archivos protegidos**

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

13. **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.

14. **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.

15. **Archivos comprometidos con el caso**

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

16. **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 un análisis temporal situación que como todos los hallazgos , debe ser consignados en el informe.

17. **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.

3.5 FASE DE DOCUMENTACION Y REPRSENTACION DE LAS PRUEBA

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 eficientey efectivo al tiempo que se reducirá las posibilidades de error a la hora de gestionar el incidente

3.5.1 UTILIZAR 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. Estos deberán ser rellenados por los departamentos afectados o por el administrador de los equipos. Alguno de los formularios que debería preparar serán:

a) Documento de custodia de la evidencia
b) Formulario de identificación del equipo y componentes
c) Formulario de incidentes tipificadas
d) Formularios de publicación del incidente
e) Formulario de recogida de evidencias
f) 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 su inicios, por lo cual serán nulas o inadmisibles en un juicio, según el Nuevo Código de podrecimiento penal (NCPP) Vigente en Bolivia.

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

I.- Los elementos de prueba solo 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: Articulo 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 procedimientos, 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, pues con este 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 Publico 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 el 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 publico 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 esta disciplina, quien en algunas casos trabajara 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 Publico 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.

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 necesitara 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.

---

9 *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 al establecido en la Constitución y en las Leyes de la república. Es único e indivisible y ejerce sus funciones de los fiscales lo representan íntegramente* ***[Ley Orgánica Ministerio Publico, Bolivia].***

NCPP – BOLIVIA: Articulo 204º.- (Pericia)

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 designara a una persona de idoneidad manifiesta.

III.-Las reglas de este Titulo regirán para los traductores e intérpretes. Mas sobre los peritos y el ordenamiento legal vigente en nuestro país.

NCPP – BOLIVIA: Articulo 205°.- (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 designara a una persona de idoneidad manifiesta.

III. Las reglas de este Titulo regirán para los traductores e intérpretes. Mas 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 debito 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 ,perdida, 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 Acta para Cadena de Custodia en el caso de Delitos informáticos indicando: fecha, hora, nombre y firma de quien recibe y de quien 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 procedimientos penal de Bolivia Art. 186.

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

I.- Regirá el procedimiento establecido para el registro. Los objetivos secuestrados serán inventarios 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 legitima, 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 ordenaran reproducciones, copias o certificación sobre su estado y serán devueltos a sus propietarios.

NCPP – BOLIVIA: Articulo 307(Anticipo de prueba)

I.- Cuando sea necesario practicar un reconocimiento, registro, reconstrucción o pericia, que por su naturaleza o característica 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 practicara 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 Procedimientos 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 esta es frágil y puede ser fácilmente alterada o destruida. Muchas veces esta alteración puede ser irreversible.

3.6.1 GARANTIZAR A CUBRIR

a) **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 ala causa, de manera que cuanto mayor sea la información que pueda obtenerse de los equipos electrónicos que se catean y asegurarse, 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.

b) **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 solo se corre el riesgo de que resulte inadmisible sino también de 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 inculpabilidad, 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 electrónicas.

NCPP – BOLIVIA: Articulo 6°.- (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 si 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 publicaran 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.

a) 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 coloco 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: Articulo 130

(Acción de Protección de privacidad)

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, hora y reputación, podrá interponer la Acción de protección de Privacidad.

La acción de protección de privacidad no procederá para levantar el secreto en materia de prensa.

CAPITULO IV

CAPITULO IV

DEMOSTRACION DE LA HIPOTESIS

4.1 DEMOSTRACION DE LA HIPOTESIS

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

4.1.1 AUTENCIDAD

La autencidad 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 autencidad entendida como aquella característica que muestra la no alterabilidad de los medios originales , busca confirmar que los registros aportados corresponden a la realidad evidenciada. Este concepto se puede apreciar claramente en todos los procedimientos:

En 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 autencidad 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 numero 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 mas para probar la autencidad 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 autencidad de los elementos probatorios adquiridos y analizad
Esto significa, que las pruebas correspondan al caso investigado sin que se de lugar a confusión, adulteración, perdida 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 autencidad de las pruebas aportadas no será refutada de acuerdo por lo dispuesto en el Art. 216 del nuevo Código de Procedimiento penal.

NCPP- BOLIVIA : Articulo 216º.- (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 esta dispuesto a declarar sobre su autencidad, sin que su negativa le perjudique.

En este caso, las partes podrán acreditar la autencidad 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 almacenamiento 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 autentificar 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 autentica

4.1.2 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 de 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, estas herramientas forenses también son utilizadas en la fase para analizar la evidencia digital y al ser con licencia no existe ninguna duda 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

4.1.3 SUFICIENCIA

La suficiencia de la evidencia o más bien , la presencia de toda la evidencia es necesaria para adelantar al 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 resultado.

En este sentido, los abogados reconocen que mientras mayores fuentes de analisi 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 esta pueda ser adquirida y de esta 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, de esta afirmación obtenemos la siguiente premisa.

q = La evidencia digital es suficiente

4.2 CONFORMIDAD CON LA LEGISLACION VIGENTE EN NUESTRO PAIS

En el procedimiento para que la evidencia digital sea legalmente, se de a conocer la normativa sobre la cual debemos basarnos para aplicar este método de análisis informático forense, dicho procedimiento se rige en el código penal de Bolivia (Art. 363 Bis y 363 Ter), Nuevo código de procedimientos penal de Bolivia y en la nueva Constitución política del Estado recientemente promulgada, es oportuno dar a conocer que muestra legislación no tiene una normativa especificada 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 enmarcadas en el "Procedimiento para que la evidencia digital sea permitida legalmente ", pues 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 este en conformidad con la legislación vigente en nuestro país, por tal afirmación obtenemos la siguiente premisa:

r= La evidencia digital esta 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 esta afirmación obtenemos:

p = La evidencia digital es autentica
q = La evidencia digital es confiable
r = La evidencia digital es suficiente
s = La evidencia digital esta en conformidad con la legislación vigente en nuestro país.

$$(p \wedge q \wedge r \wedge s) \longrightarrow$$

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 valido tenemos:

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

(p^ q^ r ^s):⟶ t // garantiza la admisibilidad de la evidencia digital

---

t

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 las premisas son verdaderas, las conclusiones también lo son:

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

Por lo tanto , como (5) es una tautología , queda demostrado que este razonamiento es válido. Con lo cual se incluye que el método de análisis informático forense garantiza la recopilación confiable de datos y evidencias digitales en situaciones jurídicas en nuestro país , pues 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 V

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

En este 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 auditoría forense para obtener la recolección de la evidencia digital 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 el 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 establecer 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 encontraría y como analizaría.
- A juicio de abogados y jueces existe desconfianza entre 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 contaminado o no. La consecuencia de no tener confianza 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 dispositivos moviles forense, pues siendo esta una nueva disciplina hace falta investigar y ampliar nuestros conocimientos en esta área.

El requerimiento de seguridad de mayor prioridad para el equipo de seguridad y auditoria 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 del método a plantear 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 método de la auditoria forense.

Además se sugiere gestionar la creación de una nueva mención dentro del pensum de la Carrera de Informática, pues es necesario la información de profesionales en el área 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

[ReEx00] Michael G. Noblett. (2000) Recovering and Examining Computer Forensic Evidence. Disponible en:
http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm
[ScWo00] Scientific Working Group on Digital Evidence (SWGDE) (2000) Digital Evidence: Standards and Principles. Disponible en:
http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm
[InfFor01] Óscar López, Haver Amaya, Ricardo León. (2001) Informática forense: generalidades, aspectos técnicos y herramientas

[ForIRT01] Antonio Javier García Martínez. (2001) LA FORMACIÓN DE UN IRT (Incident Response Team) FORENSE

[ComEvi01] Computer Evidence Defined
http://www.forensics-intl.com/def3.html
[BueAdm06] Cano Martines Jeimy José. (2006) Buenas prácticas en la administración de la evidencia digital Disponible:
http://gecti.uniandes.edu.co/docs/buenas%20practica%20evidencia%20digital%20jcano.pdf [May 2006]
[DaVa01] Brian Deering. Data Validation Using The Md5 Hash http://www.forensics-intl.com/art12.html
[JaRe96] Janet Reno, U.S. Attorney General, Oct 28, 1996

[CERT06] CERT/CC Statistics 1988-2006 Disponible en: http://www.cert.org/stats/cert_stats.html

[HBIT03] HB171:2003 Handbook Guidelines for the management of IT evidence Disponible en:

http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf

[Casey04] CASEY, Eoghan. "Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet". 2004
[EviDig05] Cano Martines Jeimy José, Mosquera González José Alejandro, Certain Jaramillo Andrés Felipe. Evidencia Digital: contexto, situación e implicaciones nacionales. Abril de 2005.
http://derecho.uniandes.edu.co/derecho1/export/derecho/descargas/texto/NasTecnologias6.pdf
Informática Forense. Juan David Gutierrez Giovanni Zuccardi

[AdmEvi03] Cano Martines Jeimy José. Admisibilidad de la Evidencia Digital: Algunos Elementos de Revisión y Análisis. Agosto de 2003. http://www.alfa-redi.org/rdi-articulo.shtml?x=1304

[Ley446] Ley 446 de Julio de 1998, http://www.sic.gov.co/Normatividad/Leyes/Ley%20446-98.php

[ElCr01] US DEPARTMENT OF JUSTICE, Electronic Crime Scene Investigation: A Guide for First Responders, 2001

[GuEvCo02] BREZINSKI, D. y KILLALEA, T. (2002) RFC 3227: Guidelines for Evidence Collection and Archiving. Network Working Group. February. Disponible: http://www.rfceditor.org/rfc/rfc3227.txt

[IOCE02]. IOCE, Guidelines for the best practices in the forensic examination of digital technology, 2002. Disponible: http://www.ioce.org/2002/ioce_bp_exam_digit_tech.html

[IOCE06]. IOCE, International Organization of Computer Evidence. Disponible: http://www.ioce.org

[FoEx04] US DEPARTMENT OF JUSTICE, Forensic examination of digital evidence. A guide for law enforcement. Special Report, 2004

[CoFor04]. INFORMATION SECURITY AND FORENSICS. Computer forensics. Part2: Best Practices, 2004 Disponible: http://www.isfs.org.hk/publications/ComputerForensics/ComputerForensics_part2.pdf

[GoPra99]. ASSOCIATION OF CHIEF POLICE OFFICERS Good practice guide for computer based evidence, 1999. Disponible: http://www.digital-detective.co.uk/documents/acpo.pdf

[NeGu03]. GODFREY, T. New Guidelines to Combat E-Crime, 2003. Disponible:http://www.saiglobal.com/newsroom/tgs/2003-09/cyberforensics/cyberforensics.htm

[Acis06] Cano Martines Jeimy José. Introducción a la informática forense. Revista ACIS Junio de 2006 Disponible en: http://www.acis.org.co/fileadmin/Revista_96/dos.pdf Informática

ANEXO A

MÉTODO DE ANALISIS FORENSE PARA LA RECOLECCION DE LA EVIDENCIA DIGITAL EN DISPOSITIVOS MOVILES

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 la Solicitud Forense, todo lo que esté involucrado con la escena del delito en este caso cajero automático.

- Solicitud video grabación del video de seguridad.

Fase de recolección de la evidencia

Utilizando wantes de látex componentes, cartones, bolsas antiestáticas.

- Se recolecciona el dispositivo movil
- (Procesos en ejecución)
- Memoria y aplicaciones del equipo .

Fase de preservación de la evidencia

Para determinar la autenticad del documento, es necesario:

- Hacer copias de la evidencia recolectada para no alterar el original y mantener su integridad.

- El valor obtenido también debe registrarse en el formulario de adquisición de evidencia digital, para demostrar la integridad y autenticad 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 tendido 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 métodos de la evidencia

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

1. Imagen de datos del dispositivo móvil.
   En este caso fue proveida junto a su marco circunstancial.

2. Verificación de integridad de la imagen del dispositivo móvil captada.
   Previamente se realizó la verificación de integridad del 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 el momento del análisis
   En un análisis de datos nunca se debe trabajar sobre la imagen original suministrada sino sobre una copia.

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

4. Identificación de las aplicaciones y el tipo del sistema operativo del equipo móvil actual.

5. Detección de información en los espacios entre la memoria interna y externa
   No existe espacio entre particiones que pueda ser analizado.

6. Identificación del sistema del incorporado (equipo móvil)
   Ya que se busca automáticamente el sistema y por esta razón pude mostrar de manera ordenada sus archivos, se debe realizar una búsqueda en el menú para identificar el tipo de sistema que tiene.

7. Recuperación de los archivos borrados
   En la recuperación inicial de la información echa, mostrándolos en el menú del equipo móvil.

8. Recuperación de información escondida
   En esta etapa se debe examinar exhaustivamente los campos reservados en el sistema de archivos y los espacios libres.

   Al igual que en la etapa , estan protegidos también se tendrán en cuenta durante la etapa de análisis de este tipo de datos.

9. Identificación de carpetas existentes

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

10. Consolidación potencialmente analizables

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

11. Analizar las aplicaciones que se tiene.
    En este caso proporcionara información suficiente para determinar la cantidad real de aplicaciones y poder incorporar otras.

12. Obtención de línea y su conexión
    En este caso no es necesario hacer una línea de tiempo ya que el mismo contara caso contrario el equipo será reconocido en mal estado .Fase de Generación del informe

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

ANEXO B

HERRAMIENTAS FORENSES

Las herramientas informáticas, son la base esencial de los análisis de las evidencias digitales en los medios informáticos. Sin embargo, estas 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 analiza por ellas sea confiable son las siguientes:

i) Mantener 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.

ii) Deben tener la capacidad de extraer un dato de la información del dispositivo.

Todo dispositivo móvil debe ser verificado, desde el comienzo hasta el final de ella sin importar si hay fragmentos en blanco.

iii) Deben tener un manejo robusto de errores de lectura. Si el proceso de copia falla del mismo tamaño y en la misma ubicación que identifique el sector que no pudo leerse, adicionalmente estas fallas deben ser documentadas.

iv) 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 se dan a conocer algunas herramientas que son utilizadas en la aplicación de la informática forense [Fernández, 2004]. El uso de herramientas para tratar la evidencia es tanto en ámbito de hardware y software. Se mencionan equipos especializados en identificación biométrica como en captura de evidencias .

Como identificación biométrica: Usados para autenticar la identidad de un equipo móvil a través de un atributo o rasgo único. Esto generalmente implica al uso de llevar . 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.

DOCUMENTACION