UNIVERSIDAD AMAZÓNICA DE PANDO

UNIVERSIDAD PRIVADA DOMINGO SAVIO

DIRECCIÓN DE POST GRADO E INVESTIGACIÓN

TESIS DE GRADO PARA OPTAR EL TÍTULO ACADEMICO DE MAGISTER EN INGENIERIA INFORMÁTICA

Metodología de Recolección de Evidencia Digital en Dispositivos móviles (celulares GSM)

POSTULANTE: Ivana Loza Rosales

Potosí-Bolivia

2012

Agradecimientos

Estos últimos años han sido para mí los más importantes, intensos y fascinantes de mi trayectoria profesional. Tiempo en que he tenido la enorme suerte de conocer y de trabajar con personas que me han ayudado a culminar con éxito este trabajo de investigación.

Mis agradecimientos a mi familia..., que me dió la fuerza y el apoyo para seguir adelante, hasta la conclusión de este trabajo de tesis, con Amor.

Todo esto no hubiera sido posible sin la guía y protección de mi Dios todopoderoso, mi único refugio y mi roca.

INDICE

CAPITULO I 1

PLANTEAMIENTO DEL PROBLEMA, OBJ. Y ESTRATEGÍA METODOLÓGICA 1

CAPÍTULO II 6

MARCO TEÓRICO 6

2.1. Informática Forense 6

2.1.1.1. Objetivos de la informática forense 8

2.2.1. Seguridad de la Información 8

2.3. Los delitos informáticos. 10

2.4. Delincuencia y criminalidad informática 11

2.5. Tipos de delitos informáticos 12

2.5.1. Tipificación de Delitos Informáticos en Colombia 14

2.5.2. Tipificación de Delitos Informáticos en Chile 15

2.5.3. Tipificación de Delitos Informáticos en Argentina 16

2.5.4. Tipificación de Delitos Informáticos en Bolivia 18

2.6.1. Recopilación de evidencia digital 23

2.7.Herramientas Forenses 25

2.7.1. Herramientas de código abierto y herramientas comerciales 26

2.7.2. Herramientas según su funcionalidad 27

2.7.3. Herramientas para la recolección de evidencia 27

2.7.4. Herramientas para el monitoreo y/o control de computadores 27

2.7.5. Herramientas de marcado de documentos 28

2.8. Procedimientos y Estándares 29

2.8.1. Recolección de evidencia 29

2.8.2. Preservación de la evidencia 29

2.8.3 Análisis de la evidencia 30

2.8.4 Presentación de un informe forense 30

2.10. Tecnología GSM 34

2.10.1. Contexto histórico de la tecnología 34

2.10.2. Infraestructura del sistema GSM 35

2.10.3. Subscriber Identity Module – SIM Card 37

2.10.4. Entendiendo los dispositivos móviles 38

2.10.4.1. BlackBerrys 39
2..10.4.2. Pocket PCs 40
2.10.4.3. Palm Handhelds 41
2.11. Teléfonos celulares 41
2.11.1. Funcionalidades 41
2.11.3. Teléfonos con Sistema Operativo Symbian 42
2.12. El Sistema Operativo Symbian 42
2.13. Modelos de Memoria 43
2.14. La tecnología GSM y los problemas de seguridad en dispositivos móviles 45
2.15. Problemas de seguridad en teléfonos celulares GSM 47
CAPÍTULO III 54
MARCO REFERENCIAL 54
3.1. Descripción del Contexto 54
3.2. Aplicación de Herramientas de Campo 61
3.2. Metodología de recolección de evidencia digital en dispositivos móviles 66
3.2.1. Fase Preparatoria 67
3.2.1.1.1. Personal de emergencia 69
3.2.1.1.2. Investigadores 69
3.2.1.1.3. Técnicos forenses 69
3.2.1.1.4. Custodios de la evidencia 69
3.2.1.1.5. Analistas forenses 70
3.2.1.2. Identificar la escena 70
3.2.1.3. Identificar el dispositivo 71
3.2.1.4. Asegurar la preservación de la evidencia 72
3.2.1.5. Determinar las herramientas forenses a utilizar 72
3.2.2. Fase de Recolección de Información 76
3.2.2.1. Recolección de evidencia 76
3.2.2.1.1. Obtención de la imagen de datos: 76
3.2.2.1.1.1. Adquisición física 76
3.2.2.1.2. Adquisición lógica 76
3.2.3. Fase de Análisis de Datos 76
3.2.3.1. Análisis de la evidencia 77
3.2.4. Reporte 78

CAPITULO IV 79
RESULTADOS 79
4.1. Realización de los escenarios de Ataque 79
4.2. Seguimiento de la Metodología Propuesta 80
4.3. Análisis de Resultados 112
CONCLUSIONES 115
RECOMENDACIONES 116
BIBLIOGRAFÍA 117

FIGURA 4. 1.SELECCIÓN DEL FABRICANTE EN LA HERRAMIENTA DEVICE SEIZURE 91
FIGURA 4. 2.SELECCIÓN DEL TIPO DE CONEXIÓN EN LA HERRAMIENTA DEVICE SEIZURE 92
FIGURA 4. 3. SELECCIÓN DEL TIPO DE DATOS QUE SE DESEAN OBTENER 92
FIGURA 4. 4.PROPIEDADES GENERALES DE LA ADQUISICIÓN DE DATOS PRIVADOS Y DE RESPALDO 95
FIGURA 4. 5. ESTRUCTURA DE LA ADQUISICIÓN DE DATOS PRIVADOS Y DE RESPALDO 95
FIGURA 4. 6. EJEMPLO DE DATOS EN FORMATO SPLITTED 96
FIGURA 4. 7. EJEMPLO DE DATOS EN FORMATO PARSED 97
FIGURA 4. 8. CAMBIO DEL LENGUAJE POR DEFECTO DE UNA APLICACIÓN 98
FIGURA 4. 9. REGISTRO DE EVENTOS ELIMINADOS DEL DISPOSITIVO 98
FIGURA 4. 10. REGISTRO DE LLAMADAS DEL DISPOSITIVO 98
FIGURA 4. 11. INFORMACIÓN DE LA LISTA DE CONTACTOS 99
FIGURA 4. 12. INFORMACIÓN DEL CALENDARIO DEL DISPOSITIVO 100
FIGURA 4. 13. INFORMACIÓN DEL REGISTRO DE LLAMADAS DEL DISPOSITIVO 100
FIGURA 4. 14. REGISTRO DE INSTALACIÓN DE APLICACIONES EN EL DISPOSITIVO 101
FIGURA 4. 15. TEXTO SOSPECHOSO ENCONTRADO BUSCANDO LA PALABRA “LOG” 102
FIGURA 4. 16. EJEMPLO DE ARCHIVO OBTENIDO BUSCANDO LA PALABRA “SYNC” 102
FIGURA 4. 17. DETALLE DEL ARCHIVO DBS_101F99FB_NSMLAGENTLOG.DB EN FORMATO SPLITTED 102
FIGURA 4. 18. DETALLE DEL ARCHIVO DBS_101F99FB_NSMLAGENTLOG.DB EN FORMATO PARSED 103
FIGURA 4. 19. CADENA DE TEXTO ENCONTRADA BUSCANDO LA MAC DEL OTRO CELULAR INCAUTADO 103
FIGURA 4. 20. PROPIEDADES GENERALES DE LA ADQUISICIÓN DEL SISTEMA DE ARCHIVOS 103
FIGURA 4. 21. ESTRUCTURA DE LA ADQUISICIÓN DEL SISTEMA DE ARCHIVOS 104
FIGURA 4. 22. IMÁGENES ENCONTRADAS EN EL TELÉFONO 106
FIGURA 4. 23. DATOS DEL PRIMER VIDEO ENCONTRADO EN EL DISPOSITIVO 106
FIGURA 4. 24. DATOS DEL SEGUNDO VIDEO ENCONTRADO EN EL DISPOSITIVO 107
FIGURA 4. 25. ARCHIVOS DE AUDIO ENCONTRADOS EN EL DISPOSITIVO 108

SÍNTESIS

El presente trabajo de investigación se trazó como objetivo, formular una metodología de recolección de evidencia digital en dispositivos móviles (celulares GSM), para proporcionar los procedimientos necesarios para obtener la mayor cantidad de detalles posibles de un incidente ocurrido en un dispositivo móvil (celular GSM) y de esta manera fortalecer la base científica del campo de informática forense en dispositivos móviles.

En base a los resultados obtenidos con la metodología de recolección de evidencia digital en dispositivos móviles (celulares GSM) se logró obtener la evidencia digital suficiente en casos ilícitos en los que se vio involucrado un dispositivo móvil (celular GSM). Se propone esta metodología como una demostración de los conocimientos adquiridos y puestos en práctica en la Maestría de Ingeniería Informática que se dictó en forma conjunta por la Universidad Amazónica de Pando y la Universidad Privada Domingo Savio.

PALABRAS CLAVE

Metodología: La palabra metodología proviene de los términos griegos método "meta" = fin, objetivo, "odos" = trayectoria senda, "logos" =tratado, ciencia o estudio; así etimológicamente metodología quiere decir "camino que debemos seguir para llegar a un fin".

Evidencia Digital: Cualquier información de valor probatorio que sea almacenada o transmitida de manera digital.

Dispositivo Móvil: Los dispositivos móviles son aparatos de pequeño tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, diseñados específicamente para una función, pero que pueden llevar a cabo otras funciones más generales.

CAPITULO I
PLANTEAMIENTO DEL PROBLEMA, OBJETIVOS Y ESTRATEGÍA METODOLÓGICA

1.1. Definición del Problema

Los dispositivos móviles, debido a su naturaleza, se prestan mucho para ser utilizados por delincuentes para realizar actos criminales, en donde se ven involucradas acciones como llamadas, almacenamiento de números telefónicos, recepción y envió de mensajes de texto entre otras. Esto para las autoridades en una investigación , es de gran importancia, pues en muchos casos se pueden recuperar dispositivos móviles, o parte de ellos, en la escena del crimen.

Existen varias alternativas para poder abordar el enfoque de la recuperación de datos, algunas de ellas, se consideran como estándares para el manejo de varios de los problemas mencionados; sin embargo, en muchos casos, puede resultar bastante difícil poner en marcha los procedimientos necesarios para dar buen rumbo a una investigación, debido a que se requiere el uso de herramientas especializadas en el tema, las cuales son costosas de adquirir, y además, exigen un entrenamiento particular para su utilización. También puede resultar complicado obtener, preservar, analizar y exponer evidencia digital relacionada con el segundo enfoque, el que está orientado a incidentes, por lo que la presente metodología que se va a desarrollar esta orientada al análisis forense dirigido a ataques informáticos en dispositivos móviles (celulares GSM).

Por tanto, y teniendo en cuenta lo anterior, esta investigación trata de dar respuesta a la pregunta: ¿Cómo realizar un análisis forense orientado a dispositivos móviles (celulares GSM)?

1.2. Objetivo General

El presente trabajo de investigación estudió la informática forense y particularmente el análisis forense en dispositivos móviles (celulares GSM).Esto con el objetivo de: Formular una metodología de recolección de evidencia digital en dispositivos

móviles (celulares GSM) para identificar y valorar las principales amenazas que atentan contra la seguridad de estos dispositivos.

1.3. Objetivos Específicos

- ✓ Compilar un marco teórico con la suficiencia necesaria para identificar y valorar las principales amenazas que atentan contra la seguridad de los dispositivos móviles (celulares GSM), lo que implica el estudio de una metodología para la recolección de evidencia digital en estos dispositivos.
- ✓ Formular una metodología para identificar y valorar las principales amenazas que atentan contra la seguridad de los dispositivos móviles (celulares GSM)
- ✓ Validar la propuesta a través de una consulta con personas que cuenten con dispositivos móviles (celulares GSM).

1.4. Hipótesis

Una respuesta al problema planteado es la: "Formulación de una metodología de recolección de evidencia digital en dispositivos móviles (celulares GSM), la cual favorecerá el esclarecimiento de los delitos informáticos en estos dispositivos"

1.5. Operacionalización de Variables

Unidad de Análisis	Variables	Definición Conceptual	Indicadores
Dispositivos Móviles	Metodología para la recolección de evidencia digital. (Causa)	Procedimiento que asegure la protección y el análisis exitoso de evidencia digital con el fin de encontrar la mayor cantidad de detalles sobre el incidente ocurrido en el dispositivo móvil.	✓ Conocimiento de informática forense. ✓ Conocimiento de la evidencia digital. ✓ Validez de la evidencia digital ✓ Utilización de Herramientas.
	Esclarecimiento de delitos informáticos (Efecto)	Aclarar un crimen genérico que agobia con operaciones ilícitas en medios informáticos.	✓ Reformas al código penal. ✓ Delitos informáticos a través de celulares en Bolivia.

El establecimiento de una metodología de recolección de evidencia digital en dispositivos móviles (celulares GSM) servirá de herramienta auxiliar a la justicia moderna la cual ayudará a enfrentar los desafíos y técnicas de los intrusos y delincuentes informáticos.

Lo que se busca con esta investigación es recopilar y analizar información con el objetivo de proponer una metodología que permita realizar un análisis forense orientado a incidentes sobre teléfonos móviles GSM, proporcionando los procedimientos necesarios para obtener la mayor cantidad de detalles posibles de un incidente ocurrido en un dispositivo celular.

La informática forense es un campo que poco a poco ha ido evolucionando; sin embargo, tiene aún muchas áreas por investigar y profundizar. Por tanto, este documento establece un conjunto de elementos conceptuales, aplicados a los dispositivos móviles GSM como una respuesta a una de las áreas que requiere hoy por hoy más investigación y profundización, dado el crecimiento tecnológico que se presenta actualmente, de esta manera, fortalecer la base científica del campo de informática forense en dispositivos móviles.

Finalmente el aporte práctico radica en que la formulación de una metodología de recolección de evidencia digital en dispositivos móviles (celulares GSM) coadyuvará a la identificación de delitos informáticos brindando un ambiente de trabajo acorde a las exigencias tecnológicas.

Los métodos de Nivel Teórico, posibilitan la interpretación conceptual de los datos.

La recopilación de información histórica aportó de forma significativa al presente trabajo de investigación. El estudio del comportamiento histórico da una base sobre la cual comenzar a analizar y "explicar" por qué se utilizó una u otra herramienta para la recolección de evidencia digital en dispositivos móviles (celulares GSM). Los datos históricos no dan una explicación en sí, sino que debe interpretar lo que ocurrió y por qué ocurrió.

El método sistémico durante el desarrollo de la investigación contempla las siguientes tareas: seleccionar y relacionar componentes, formular acciones y procesos para realizarlos, con una planificación y orden, de interdependencia y con procesos de retroalimentación.

Mediante los métodos empíricos se recopiló el mayor número de datos los que permitieron alcanzar los objetivos de la investigación. Para este estudio se utilizó como herramienta la entrevista, realizada a algunas personas relacionadas con el tema, para iniciar la etapa de análisis de requerimientos y para realizar un diagnóstico de la situación actual y determinar algunas necesidades en el área.

En el capítulo I se hizo referencia al planteamiento del problema, objetivos y estrategia metodológica, esto para lograr una adecuada comprensión de lo que se pretende alcanzar con el presente trabajo de investigación.

En el capítulo II se propuso las teorías utilizadas en el trabajo de investigación, es decir, se considerara los elementos del marco teórico.

En el capítulo III se realizara una descripción de los procedimientos estándar que se deben seguir para asegurar la protección y análisis exitoso de la recolección de evidencia digital en dispositivos móviles (celulares GSM), con el fin de encontrar la mayor cantidad de detalles sobre el incidente ocurrido en el dispositivo. Revisar con detenimiento los procedimientos y estándares establecidos en la actualidad contribuirá a considerar las mejores prácticas y fases expuestas, generando con ello una metodología para la recolección de evidencia digital en dispositivos móviles GSM.

En el capítulo IV se realizó la validación de la propuesta, así como la descripción del seguimiento que se realizó a la misma. Se concluye con las recomendaciones y conclusiones.

Capítulo II

MARCO TEÓRICO

2.1. Informática Forense

"Es fácil imaginar que la informática forense tiene que ver con los programas o aplicaciones que se utilizan en la medicina forense, pero en realidad de lo que se trata es de la investigación penal, con el fin de resolver problemas online.

Con el auge de las computadoras y las Tecnologías de Información, la seguridad informática está cada vez más afectada, lo que ha favorecido de alguna manera la implementación de una serie de acciones que refuerzan la seguridad, sin embargo no han sido suficientes ya que los delincuentes informáticos encuentran nuevas formas para continuar con sus acciones.

La informática forense surgió o dio sus primeros pasos aproximadamente hace 25 años en Estados Unidos, cuando el FBI se dio cuenta que los criminales empezaron a usar la tecnología para cometer sus crímenes.

En 1984 el FBI inicio un programa llamado el Programa de Medios Magnéticos que dio origen al CART, un equipo de análisis computacional. En 1988 Michael Anderson un agente del IRS (servicio de rentas internas), armó un grupo de especialistas y se reunieron con 3 compañías involucradas en la recuperación de datos, compañías que luego se convirtieron en Symantec.

En una de estas reuniones se crearon las clases de Especialistas de Recuperación de Evidencia Computacional, en 1988 y 1989 en el centro de entrenamiento federal FLETC, y también se creó la IACIS, Asociación Internacional de Especialistas en la Investigación Computacional." *(SHEL ,1997:10).*

"Entre 1993 y 1995 junto con el Departamento de Hacienda de Canadá se formó el programa CIS para incluir a todas las agencias de la tesorería estadounidense en el entrenamiento. Al mismo tiempo se formó la IOCE, Organización Internacional en Evidencia Computacional, cuyo propósito es proveer un foro internacional para el

intercambio de la información relacionada con la investigación computacional y la informática forense.

Para ese entonces la informática forense ya se había consolidado como un campo vital en el área de la investigación, y que a medida que la tecnología avanzaba de forma acelerada así tenían que hacerlo las organizaciones encargadas de la informática forense.

Para el 2003 el CART trabajaba en 6500 casos y estaba examinando 782 Terabytes de datos.

Actualmente las compañías de Software producen software forense más robusto y los agentes de la ley y militares entrenan a más personal para responder a los crímenes que involucren tecnología.

La informática forense está adquiriendo gran importancia dentro del área de la información electrónica, esto debido al aumento del valor de la información y al uso que se hace de la misma; la computadora y los sistemas informáticos son fundamentales dentro de esta sociedad moderna y por lo tanto favorecen al crecimiento de una organización.

Lastimosamente estas mismas herramientas están siendo utilizadas para cometer delitos, pero igual que un crimen en la dimensión física deja evidencias, aquí también se deja evidencias del crimen, pero dichas evidencias quedan almacenadas de forma digital, en la mayoría de los casos dicha información no se puede leer o recolectar por medios comunes o mecanismos tradicionales. Es de aquí que nace el estudio de la informática forense, que provee el conocimiento y los instrumentos para estudiar y solucionar este nuevo tipo de delitos.

Incluso es posible resaltar su carácter científico, ya que tiene sus fundamentos en las leyes de la física, de la electricidad y del magnetismo, por ejemplo podemos destacar que es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer y recuperar la información aunque haya sido eliminada.”(SHEL 1997:12)

Si a todo esto se le aplica un método científico, con procedimientos estrictos, en donde se aplique la recolección, análisis y validación de todo tipo de pruebas digitales, puede fácilmente ayudar a resolver varios crímenes. Es así que la informática Forense se puede considerar como una ciencia que permite la extracción, manipulación y el análisis de evidencias.

2.1.1.1. Objetivos de la informática forense

"Como disciplina, la informática forense tiene como fin el aplicar los estándares y procedimientos estándar que se utilizan en una investigación de crímenes e incidentes, para enfocarlos hacia el análisis de datos y evidencia digital, todo esto soportado por herramientas tecnológicas de extracción y análisis de datos." (SHEL ,1997:17).

2.2. Seguridad

"La seguridad es una serie de costos de oportunidad donde se debe balancear la seguridad con la utilización y el costo. La seguridad es inversamente proporcional a la utilización y el costo. Conforme un sistema se vuelve más seguro, este se vuelve mas estrictivo y difícil de utilizar. Por lo tanto, el costo de administrar y mantener un sistema puede subir significativamente. Alcanzar un novel apropiado de seguridad para un sistema implica un balanceo delicado de protección y costo.

Las amenazas a los sistemas de información y la batalla para protegerlos son como la guerra de guerrillas. La guerrilla usa tácticas ocultas para mirar y sabotear su sistema. El enemigo es usualmente desconocido y se preocupa de cubrir su rastro para poder atacar de nuevo sin problemas. En algunos casos, la guerrilla obtiene información necesaria para acceder a sus sistemas de sus propios empleados de confianza. En algunos casos, la guerrilla es el empleado de confianza." (SHEL, 1997 : 36-37).

2.2.1. Seguridad de la Información

"La seguridad en la información es la práctica de proteger los recursos y los datos de un sistema de computadoras y redes, incluyendo la información guardada en dispositivos de almacenamiento y en su transmisión.

Las amenazas de seguridad son tanto naturales como intencionales. Los datos de los sistemas son vulnerables tanto a desastres naturales como a la corrupción creada por gente maliciosa. Inundaciones, fuego, competidores, gobiernos extranjeros, personas vengativas -o solo curiosas-, y muchos pueden ser la fuente. Un ataque perpetrado por humanos puede ser tanto activo como pasivo."(CHAPM : 4).

- "Los ataques activos tratan realmente de cambios en los datos almacenados o transmitidos. Puede consistir incluso en el borrado, la corrupción, el retraso o el atasco de transmisiones. Los ataques activos pueden aparentar ser accidentes.
- Los ataques pasivos tratan de la recolección de información sin que nadie sepa que se está produciendo. Las escuchas y los pinchazos electrónicos son ejemplo de ellos. La información con frecuencia se usa para atacar un sistema más importante." (SHELL ,1997: 36-37).

El NIST (National Institute for Standards and Techonology, Instituto Nacional para Estándares y Tecnología, de los Estados Unidos) ha resumido los siguientes estándares de seguridad que se refieren como los requerimientos funcionales mínimos de seguridad para sistemas operacionales multiusuario:

- Identificación y autentificación: la identificación y la verificación de usuarios se realizan a través de un procedimiento de inicio de sesión y la autorización de uso de otros sistemas se basa en este tema de seguridad.
- Control de Accesos: los derechos y permisos que controlan como usuarios pueden acceder a los recursos y archivos de la red.
- Control de cuenta y de auditoría: un sistema de registro y control de los inicios de sesión de las actividades en los sistemas de red y los enlaces entre ellos y las cuentas de usuarios específicos.
- Reutilización de objetos: métodos para suministrar a múltiples usuarios la posibilidad de acceder a recursos individuales.
- Precisión: métodos para proteger los recursos frente a errores, corrupción y accesos autorizados.

- Fiabilidad: métodos para asegurarse de que los sistemas y los recursos estén disponibles y para protegerlos frente a fallos o pérdidas.
- Intercambio de datos: métodos para asegurar las transacciones de datos con canales de comunicaciones externas e internas. (CHAPM :4).

  En relación con los datos y sus características Chapman y Zwicky mencionan que estos tienen tres características que deben protegerse:
- Confidencialidad: haciendo alusión a que quizá una persona no quiere que otras personas los conozcan.
- Integridad: es muy probable que el dueño de los datos no quiera que otras personas los cambien.
- Disponibilidad: con seguridad el usuario dueño de los datos quiere utilizarlos el mismo.

Las personas tienden a enfocarse en los riesgos asociados con mantenerlos en secreto, y es cierto que por lo general son grandes riesgos.

2.3. Los delitos informáticos.

El progreso tecnológico que ha experimentado la sociedad, supone una evolución en las formas de infringir la ley, dando lugar, tanto a las diversificaciones de los delitos tradicionales como la aparición de nuevos actos ilícitos. Esta situación ha motivado un debate en torno a la necesidad de diferenciar o no los delitos informáticos del resto y de definir su tratamiento dentro del marco legal.

María de la Luz Lima indica que el delito electrónico en un sentido amplio es "cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin", y que en un sentido estricto, el delito informático, es "cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin". (María de la Luz Lima, "Delitos Electrónicos":100).

Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo que en la forma típica son "las conductas típicas, antijurídicas y culpables

en que se tienen a las computadoras como instrumento o fin" y la forma atípica "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin". (Julio Téllez Valdés, "Derecho Informático":43).

El Convenio de Cyber-delincuencia del Consejo de Europa, define a los delitos informáticos como "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas redes y datos"

Conviene destacar entonces, que diferentes autores y organismos han manifestado diferentes apreciaciones para señalar las conductas ilícitas en las que se utiliza la computadora, esto es "delitos informáticos", "delitos electrónicos", "delitos relacionados con la computadora", "crímenes por computadora", "delincuencia relacionada con el computador".

Tal como podemos notar en las definiciones establecidas por autores anteriores, no existe una definición de carácter universal propia de delito informático, sin embargo, debemos resaltar que han sido los esfuerzos de especialistas que se han ocupado del tema y han expuesto conceptos prácticos y modernos atendiendo entornos nacionales concretos, pudiendo encasillar parte de los temas en esta área de la criminalística. Es preciso señalar que la última definición brindada por el Convenio de Cyber-delincuencia del Consejo de Europa anota especial cuidado en los pilares de la seguridad de la información: la confidencialidad, integridad y disponibilidad.

2.4. Delincuencia y criminalidad informática

Carlos Sarzana (1998:20), describe en su obra "Criminalitá e Tecnología", que los crimines por computadora comprenden "cualquier comportamiento criminógeno, en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como un simple símbolo", entonces según esta descripción las personas que cometen delitos o crímenes informáticos, están enmarcadas dentro de lo

que se conoce como criminología, y la investigación de dichos delitos, están sujetos a las ciencias de la criminalística.

Es preciso que se reconozca la diferencia entre la criminología y la criminalística; La criminología trata de investigar el por qué y que fue lo que llevo al individuo a cometer el delito, mientras que la criminalística según Montiel Sosa (1998:86) , se definen como "una ciencia multidisciplinaria que reúne conocimientos generales, sistemáticamente ordenados, verificables y experimentables, a fin de estudiar, explicar y predecir el cómo, dónde, cuándo, quién o quienes los cometen" , la criminalística al ser multidisciplinaria se aplica en temas de balística, medicina forense, física, química, e incluso la informática, entre otras, y se apoya de métodos y técnicas propias del trabajo de las diferentes disciplinas.

2.5. Tipos de delitos informáticos

La tipificación o clasificación de los delitos procura, salvaguardar los bienes jurídicos. Los bienes jurídicos son intereses relevantes de las personas en tantos sujetos sociales, considerados especialmente valiosos, dignos de protección penal frente a conductas que los dañen o ponen en peligro, entonces por ejemplo: con respecto al delito del hurto, el bien jurídico es la propiedad; en caso del delito de homicidio el bien jurídico protegido es la vida; y, en el caso de las nuevas tecnologías el bien jurídico protegido es la información.

Muchos autores y organismos han clasificados de diferentes maneras los tipos de delitos informáticos según diferentes criterios, coincidiendo entre los principales los siguientes:

Reconocidos por las Naciones Unidas	Abogados especializados en delitos informáticos
Fraudes mediante la manipulación de computadoras (programas, datos de entrada y salida, repetición automática de procesos).	Fraudes mediante la manipulación de computadoras: 1. Delitos contra elementos físicos-hardware (rabo, estafa). 2. Delitos contra elementos lógicos (daños, accesos ilícitos a sistemas, acceso ilícito a datos, protección de programas)
Falsificaciones informáticas (alteración de documentos falsificación de documentos.	
Daños o modificaciones de programas o datos computarizados (sabotaje, virus, bombas lógicas)	Delitos cometidos a través de sistemas informáticos: 1. Estafas 2. Apoderamiento de dinero por tarjetas de cajero. 3. Uso de correo electrónico con finalidad criminal. 4. Utilización de internet y dispositivos móviles (celulares) como medio criminal.
Acceso no autorizado a servicios y sistemas informáticos (piratas, reproducción no autorizada).	

Tipificación de delitos informáticos

Fuente: Organización de las Naciones Unidas

Fuente:http://informática-juridica.com

Tomando como referencia la clasificación o tipificación de los delitos informáticos, éstos se clasifican de la siguiente manera:

1. **Fraudes:-** Delitos de estafa a través de la maniobra de datos o programas para la obtención de un lucro ilícito (caballos de troya, falsificaciones, etc.).
2. **Sabotaje informático.-** Daños mediante la destrucción o modificación de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos (bombas lógicas, virus informáticos, malware, ataques de negación de servicio, etc.).

3. **Espionaje informático:** Divulgación no autorizada de datos reservados
4. **Pornografía Infantil:** Inducción, promoción, producción, venta, distribución facilitamiento de prostitución, cuando se utilizan menores con fines de exhibicionistas o pornográficos.
5. **Infracciones de Propiedad Intelectual:** Copia o reproducción no autorizada de programas informáticos de protección legal.

2.5.1. Tipificación de Delitos Informáticos en Colombia

En lo referido a delitos informáticos Colombia con el objetivo de penalizar estos promulga la Ley 1273 por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado-Denominado "De la protección de la información y de los datos". Y se preservan integralmente los sistemas que utilicen tecnologías de la información y las comunicaciones, entre otras disposiciones.

Artículo 1°. Adicionarse el Código Penal con un título VII BIS denominado "De la protección de la información y de los datos", del siguiente tenor:

CAPÍTULO PRIMERO

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que , sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legitimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269B: OBSTECULACIÓN ILEGÍTIMA DEL SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de

telecomunicaciones, incurrirá en pena de prisión cuarenta y ocho (48) a noventa meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con un pena mayor.

Artículo 269 C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS: El que sin orden judicial previa intercepte datos informáticos en su orden, destino o en el interior de sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269 D: DAÑO INFORMÁTICO: El que sin estar facultado para ello. Destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

2.5.2. Tipificación de Delitos Informáticos en Chile

Chile promulga la Ley 19223 relativa a Delitos Informáticos

Artículo 1º.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2º.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3º.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4º.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.

2.5.3. Tipificación de Delitos Informáticos en Argentina

Sin duda alguna el país vecino de la Argentina también está involucrado en la lucha contra el crimen tecnológico, es así que realizó la modificación e inserción de las siguientes figuras: Pornografía infantil por Internet u otros medios electrónicos (art. 128 CP); Violación, apoderamiento y desvío de comunicación electrónica (art. 153, párrafo 1º CP);Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (art. 153, párrafo 2º CP); Acceso a un sistema o dato informático (artículo 153 bis CP); Publicación de una comunicación electrónica (artículo 155 CP); Acceso a un banco de datos personales (artículo 157 bis, párrafo 1º CP);Revelación de información registrada en un banco de datos personales (artículo 157 bis, párrafo 2º CP); Inserción de datos falsos en un archivo de datos personales (artículo 157 bis, párrafo 2º CP; anteriormente regulado en el artículo 117 bis, párrafo 1º, incorporado por la Ley de Hábeas Data); Fraude informático (artículo 173, inciso 16 CP);Daño o sabotaje informático (artículos 183 y 184, incisos 5º y 6º CP).
El texto de la mencionada ley en Extenso es:

Art. 1. - Incorpóranse como últimos párrafos del artículo 77 del Código Penal, los siguientes: El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

Art. 2. - Sustitúyese el artículo 128 del Código Penal, por el siguiente: Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a

actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores. Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

Art. 3. - Sustituyese el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, por el siguiente: "Violación de Secretos y de la Privacidad"

Art. 4. - Sustituyese el artículo 153 del Código Penal, por el siguiente: Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

Art. 5. - Incorpórase como artículo 153 bis del Código Penal, el siguiente: Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un (1) mes a un (1) año de prisión cuando el

acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

2.5.4. Tipificación de Delitos Informáticos en Bolivia

En el tema de legislación de los delitos informáticos, en Bolivia se está un poco atrasado, solo se tiene dos delitos tipificados. Se tiene manipulación informática y acceso indebido en el Código Penal.

Lo lamentable es que el acceso indebido no tiene cárcel. Sin embargo de estas debilidades de nuestra legislación, cabe mencionar que estos delitos cuando se cometen, casi siempre van de la mano de otros delitos antiguos y ya tipificados en el Código Penal.

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

Articulo 363.- ter (ALTERACION, ACCESO Y USO INDEBIDO DE DATOS INFORMATICOS). El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días."

Existen también dentro de la NUEVA CONSTITUCION POLITICA DEL ESTADO, dos Artículos referentes al tema de Delitos Informáticos, que dicen:

SECCIÓN III

ACCIÓN DE PROTECCIÓN DE PRIVACIDAD

Artículo 133

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

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

Artículo 134

I. La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional.

II. Si el tribunal o juez competente declara procedente la acción, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado.

III. La decisión se elevará en revisión de oficio ante el Tribunal Constitucional Plurinacional, en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ello se suspenda su ejecución.

IV. La decisión final que conceda la Acción de Protección de Privacidad será ejecutada inmediatamente y sin observación. En caso de resistencia se procederá de acuerdo a lo señalado en la Acción de Libertad. La autoridad judicial que no proceda conforme a lo dispuesto por este artículo, quedará sujeta a las sanciones previstas por la ley.

Al respecto también la Asamblea Legislativa Plurinacional, ha sancionado la siguiente Ley:

LA ASAMBLEA LEGISLATIVA PLURINACIONAL,

DECRETA:

LEY GENERAL DE TELECOMUNICACIONES,

TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

CAPÍTULO SEGUNDO

GOBIERNO ELECTRÓNICO Y SOFTWARE LIBRE

El Órgano Ejecutivo del nivel central del Estado, elaborará los lineamientos para la incorporación del Gobierno Electrónico.

Artículo 77. (SOFTWARE LIBRE).

I. Los Órganos Ejecutivo, Legislativo, Judicial y Electoral en todos sus niveles, promoverán y priorizarán la utilización del software libre y estándares abiertos, en el marco de la soberanía y seguridad nacional.

II. El Órgano Ejecutivo del nivel central del Estado, elaborará el plan de implementación de software libre y estándares abiertos en coordinación con los demás órganos del Estado y entidades de la administración pública.

Artículo 78 : Tienen validez jurídica y probatoria:

I. El acto o negocio jurídico realizado por persona natural o jurídica en documento digital y aprobado por las partes a través de firma digital, celebrado por medio electrónico u otro de mayor avance tecnológico.

II. El mensaje electrónico de datos.

III. La firma digital.

Artículo 83. (CERTIFICADOS DIGITALES PARA EL SECTOR PÚBLICO).

La Agencia para el Desarrollo de la Sociedad de la Información en Bolivia – ADSIB, prestará el servicio de certificación para el sector público y la población en general a nivel nacional, conforme a las normas contenidas en la presente Ley, y velará por la autenticidad, integridad y no repudio entre las partes.

Artículo 84. (REGLAMENTACIÓN).

El reglamento referido a firmas y certificados digitales comprenderá:

1. Los requisitos, funciones, procedimientos, convenio de partes, obligaciones, cese de la entidad certificadora autorizada, responsabilidad de las entidades certificadoras autorizadas ante terceros, sanciones, resolución de controversias y otros.
2. La publicidad, seguridad e integridad en el uso de la firma digital.
3. Las definiciones, principios y procedimientos relativos al tratamiento de los datos personales.

CAPÍTULO QUINTO
CORREO ELECTRÓNICO

Artículo 89. (CORREO ELECTRÓNICO PERSONAL).

A los efectos de esta Ley el correo electrónico personal se equipara a la correspondencia postal, estando dentro del alcance de la inviolabilidad establecida en la Constitución Política del Estado. La protección del correo electrónico personal abarca su creación, transmisión, recepción y almacenamiento.

Artículo 90. (CORREO ELECTRÓNICO LABORAL).

Cuando una cuenta de correo electrónico sea provista por la entidad empleadora al dependiente como medio de comunicación, en función de una relación laboral, se entenderá que la titularidad de la misma corresponde al empleador, independientemente del nombre de usuario y clave de acceso que sean necesarias para su uso, debiendo comunicarse expresamente las condiciones de uso y acceso del correo electrónico laboral a la empleada o empleado.

Artículo 91. (COMUNICACIONES COMERCIALES PUBLICITARIAS POR CORREO ELECTRÓNICO O MEDIOS ELECTRÓNICOS)

Mediante reglamento se establecerán, las condiciones de las comunicaciones comerciales publicitarias realizadas por medio de correo electrónico o cualquier otro medio electrónico, sin perjuicio de la aplicación, en los casos que corresponda, de la normativa vigente en materia comercial sobre publicidad y protección a las usuarias o usuarios

2.6. Evidencia digital

De acuerdo a la conceptualización de Eoghan Casey (1997:9) “la evidencia digital es un tipo de evidencia física. Esta construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales”.

Miguel López Delgado (1998:13), define la evidencia digital como “el conjunto de datos en formato binario, esto es, comprende los ficheros, su contenido o referencia a estos (metadatos) que se encuentran en los soportes físicos o lógicos del sistema vulnerado o atacado.”

Según Jeimy J. Cano M., (“Introducción a la Informática Forense”, Revista Sistemas N° 96) “la evidencia digital es la materia prima para los investigadores, donde la tecnología informática es parte fundamental del proceso. La evidencia digital posee, entre otros, los siguientes elementos que la hacen un constante desafío para aquellos que la identifican y analizan en la búsqueda de la verdad: Es volátil, es anónima, es duplicable, es alterable y modificable, es eliminable. Estas características advierten sobre la exigente labor que se requiere por parte de los especialistas en temas de informática forense, tanto en procedimientos, como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia presente en una escena del delito. Además, revela con respecto al tratamiento de la evidencia digital, que se debe guardar especial cuidado a: su debido registro, admisibilidad, valor probatorio, preservación transformación y recuperación.”

Con estos argumentos, la evidencia digital, es un insumo de especial cuidado, para el proceso de investigación de delitos informáticos, que debe ser tratada por parte de los especialistas, tratando de conservar todas las medidas de precaución necesarias para no contaminarla y que sea objeto de desestimación ante un proceso litigioso.

Elemento indispensable para el inicio de una investigación, conjunto de datos binarios los cuales una vez traducidos ayudan al encuentro de la verdad.

2.6.1. Recopilación de evidencia digital

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

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

2) En el caso de que se elija la segunda alternativa y el profesional se encuentra capacitado para realizarlo, se debe iniciar con el proceso de recopilar las evidencias que permitan determinar los métodos de entrada, actividades de los intrusos, identidad y origen, duración del evento o incidente, siempre precautelando evitar alterar las evidencias durante el proceso de recolección.

Hay que asegurarse de llevar un registro de cada unos 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.

Durante esta fase, es recomendable utilizar una técnica o metodología de recolección de evidencias, para ello, el profesional debe hacer uso de prácticas o metodologías que sean reconocidas y que sobretodo puedan ser reproducidas o replicadas, bajo el mismo contexto del escenario presente.

Para la recolección de evidencias se dispone de marcos de trabajo de distribución libre que han sido desarrollados tomando en cuenta las mejores prácticas. A continuación la siguiente tabla lista algunas de las guías de reconocimiento mundial, para la recolección de evidencias en computación forense:

GUIA	PATROCINADOR	DISTRIBUCION
RFC 3227-Guia para recolectar y archivar evidencia.	Network Working Group	Libre
Guia IOCE- Guia de mejores practicas en el examen forense de tecnología digital.	International Organization on Computer Evidence	Libre
Guía DoJ1 - Investigación en la escena del crimen electrónico	U.S. Department of Justice	Libre
Guía DoJ2 - Examen forense de evidencia digital	U.S. Department of Justice	Libre
Guía Hong Kong Computación forense – Parte 2 – Mejores Practicas	SWGDE - Scientific Working Group on Digital Evidence	Libre
Guía Reino Unido - Guía de Buenas prácticas para evidencia basada en computadoras.	ACPO - Association of Chief Police Officers	Libre
Guía Australia - Guía para el manejo de evidencia en IT	Estándar Australiano	No Libre

Guías de mejores prácticas de computación forense

Fuente:http://informática-juridica.com

Fuente: Organización de las Naciones Unidas

2.7. Herramientas Forenses

En la actualidad se encuentran disponibles varias herramientas para recuperar evidencia. El uso de herramientas detalladas y completas se hace necesario debido a:

• La gran cantidad de datos que se pueden almacenar en un computador en la actualidad; sin estas herramientas la búsqueda de las mismas sería muy dispendiosa y poco eficiente.

• La variedad de formatos de archivo. Las herramientas de recolección de evidencia ayudan a la identificación de los diferentes tipos de archivos que se recuperan, facilitando de la misma manera el análisis de los datos.

• La necesidad de recopilar información de una manera exacta. Las herramientas asisten en la recuperación de la evidencia digital sin alterarla o borrarla del disco duro.

• La necesidad de verificar que la copia es exacta. Las herramientas de recolección de evidencia pueden obtener un *hash* de la imagen del disco para verificar que la copia es exacta bit a bit al momento del análisis forense, esto sería imposible de realizar de forma manual.

• Limitaciones de tiempo para analizar toda la información. Las herramientas forenses agilizan el proceso de análisis permitiendo búsqueda de palabras clave dentro de un gran conjunto de datos, entre otras características que hacen que el proceso investigativo sea más rápido.

• Facilidad para borrar archivos de computadores. Las herramientas de recolección de evidencia asisten en la recuperación de archivos y/o directorios borrados en el sistema.

Basado en lo anterior, se concluye que las herramientas forenses son de gran ayuda en cuanto a recolección y análisis de evidencia se refiere, protegiendo la integridad y facilitando la disponibilidad de la información. En este contexto los análisis forenses pueden adelantarse como se enuncia a continuación:

a. Utilizando de manera correcta y efectiva las herramientas del sistema operativo que estamos investigando y/o las propias del kit de herramientas que pertenece al plan de

respuesta ante incidentes. Esta opción resulta poco efectiva ya que cada vez los atacantes emplean herramientas más sigilosas y perfeccionadas para realizar sus ataques.

b. Utilizando un conjunto de herramientas específicas para el análisis de evidencias. Esta opción resulta mucho más eficaz ya que permite realizar la investigación de una manera más eficiente obteniendo mejores resultados.

En el conjunto de herramientas específicas encontramos dos formas de clasificación:

a. Comerciales y no comerciales: En la actualidad existen tanto herramientas comerciales no gratuitas como es el caso de EnCase de la empresa Guideance Software como herramientas de código abierto (*Open Source*), las cuales se pueden descargar libremente desde la página de sus correspondientes autores o miembros del proyecto.

b. Clasificación de acuerdo a su funcionalidad: En esta categoría se encuentran cuatro grupos principales los cuales son: Herramientas para la recolección de evidencia, herramientas para el monitoreo y/o control de computadores, herramientas de marcado de documentos y herramientas de hardware.

2.7.1. Herramientas de código abierto y herramientas comerciales

Una forma de clasificación de las herramientas forenses es de acuerdo a su distribución. En el mercado existen actualmente herramientas de código abierto y herramientas comerciales. Las herramientas de código abierto son aquellas que están disponibles de forma gratuita en Internet y de las cuales se encuentra en código fuente también publicado en la red, el cual puede ser modificado y mejorado según las necesidades del usuario. Por otro lado, las herramientas comerciales son aquellas que son diseñadas por empresas las cuales recaudan una cantidad de dinero específica para que el usuario obtenga una licencia, la cual proporciona beneficios como soporte técnico y actualizaciones durante cierto tiempo.

2.7.2. Herramientas según su funcionalidad

Otra forma de clasificar las herramientas forenses existentes en la actualidad es de acuerdo a su funcionalidad. Si bien es cierto que todas las herramientas descritas están enfocadas en la disciplina de la informática forense, no todas se especializan en el mismo campo. A continuación se definen los grupos de herramientas para: Recolección de evidencia, monitoreo y/o control de computadores, marcado de documentos y herramientas de hardware. Finalmente, se exponen algunas de las herramientas existentes actualmente, las cuales realizan la funcionalidad especificada en el nombre del grupo de clasificación.

2.7.3. Herramientas para la recolección de evidencia

Las herramientas para recolección de evidencia son las más comunes en el mercado y, a la vez, son las más completas ya que no solo se dedican a recolectar la información sino que ayudan a facilitar el análisis de la evidencia permitiendo potentes búsquedas, realizando data carving en búsqueda de archivos, descifrando contraseñas, permitiendo el acceso al slack space4 y al espacio unallocated para finalmente mostrar los resultados obtenidos de forma comprensible.

2.7.4. Herramientas para el monitoreo y/o control de computadores

Las herramientas forenses que clasifican para esta categoría son utilizadas para obtener información sobre el uso de la maquina sospechosa y recolectar dicha información para después ser utilizada como evidencia digital en una investigación especifica. Las herramientas de esta categoría se diferencian por su complejidad que van desde recolectar información del teclado hasta tomar el control total del computador de forma remota.

En el nivel de menor complejidad encontramos los keyloggers los cuales “son programas para el espionaje que plantean muchos problemas éticos y legales”. Entre estos problemas se encuentra el robo de información susceptible en café Internet y en general en sitios de acceso publico a Internet. La información puede ir desde datos personales hasta contraseñas de correo electrónico y números de tarjeta de crédito.

Actualmente “hay indicios de que entre los delincuentes electrónicos mundiales la pesca *phising* quizá esté ya pasada de moda. En algunos países, como Brasil, ha sido eclipsada por una forma aún más virulenta de estafa electrónica: El uso de programas de detección de pulsaciones (*keyloggers*) que copian en silencio lo que teclean los usuarios del ordenador y envían la información a los estafadores.” Debido a este uso indebido de la herramienta, la mayoría de estos programas son detectados automáticamente por la mayoría de antivirus actuales como Malware incluyéndolos en la categoría de troyanos.

Actualmente existen varios de estos programas “legales” los cuales son frecuentemente usados por padres de familia que sean saber las actividades de sus hijos en Internet, entre otros usos espía. Un ejemplo de una empresa líder en este tipo de software es Amecisco Inc, fundada en 1997 y la cual tiene KeyLoggers tanto de software como de Hardware. La diferencia entre estos dos tipos de keyloggers es que el primero puede venir instalado físicamente en el teclado del equipo mientras que el segundo es un software que se instala en el Sistema Operativo y queda invisible para el usuario.

2.7.5. Herramientas de marcado de documentos

Existen en el mercado programas que permiten marcar el software para que, en caso de robo de información, sea posible detectarlo fácilmente. “Algunos sitios en Internet que manejan información confidencial o sensitiva, tienen mecanismos para validar el ingreso, pero, debido a que no existe nada como un sitio 100% seguro, se debe estar preparado para incidentes”.

Cuando se expone el concepto de “robo de información” no se refiere solamente al robo de software sino también al robo de imágenes, música, videos y documentos. Desde luego este robo es perpetuado en obras digitales y es por esto que existe este tipo de herramientas de marcado de documentos las cuales utilizan la tecnología llamada comúnmente “*Digital Watermarking*” o marcas de agua digitales.

Los orígenes de esta tecnología vienen de otra técnica anterior llamada esteganografía (en inglés *steganography*). “La esteganografía no nació con la intención de proteger el

copyright, ni mucho menos. Su utilidad básica no es otra que la de proteger la información. Cuando se trata de proteger la información, esta se puede cifrar". Para ilustrar mejor el uso de esta técnica se expone el siguiente escenario: Se desea enviar información confidencial a un determinado país en donde los derechos humanos son casi inexistentes. La persona que recibe dicha información puede resultar en prisión por el solo hecho de venir cifrada, aunque en realidad ni se conozca el contenido. "Esa es la utilidad real de la esteganografía: Cifrar esta información y enviarla camuflada dentro de un archivo de otro tipo, como puede ser una imagen, un fichero de sonido o un texto".

2.8. Procedimientos y Estándares

A continuación se expone un procedimiento estándar que permite efectuar una investigación forense digital procurando fortalecer la admisibilidad y validez de las evidencias digitales encontradas en el contexto del incidente, con el fin de presentarlas como elementos materiales probatorios en un proceso jurídico. El procedimiento consiste en:

2.8.1. Recolección de evidencia

En esta fase del procedimiento, lo primero que se debe realizar es un análisis del sistema o periférico que posiblemente se encuentre involucrado en el incidente.

2.8.2. Preservación de la evidencia

En esta fase del proceso se debe realizar la preservación de los datos y dispositivos de una manera rigurosa debido a que si no se realiza de esta manera, es posible que la evidencia pierda su carácter de admisible desde el punto de vista legal. Es importante resaltar que en este proceso de preservación se debe ser estricto con los procedimientos a la hora de tratar con la evidencia por parte de agentes externos, más precisamente, las personas que la manipulen.

2.8.3 Análisis de la evidencia

En esta fase de la investigación, se pueden encontrar grandes cantidades de información, que según el tipo de ataque o suceso que se produjo durante el incidente, puede acarrear gran tiempo de la investigación, en procesos como reconstrucción de la evidencia, e identificación de acciones puntuales. En esta fase, seguramente se requerirá que haga uso de un *toolkit* especializado, para que no se produzcan cambios en la evidencia original, y facilite el trabajo del investigador, para encontrar más fácilmente rastros y producir informes de forma clara y precisa.

2.8.4 Presentación de un informe forense

Finalmente culmina la investigación y en este paso se presentan los resultados por parte del investigador sobre su búsqueda y análisis de los medios, lo que se encontró en la fase de análisis de la evidencia, así como información puntual de los hechos previamente sugeridos para investigar y posibles responsables, etc.

2.9. Estándares y procedimientos de acuerdo a la ACPO

The Association of Chief Police Officers (ACPO) Good Practice Guide for Computer Based Electronic Evidence [ACPO] sugiere cuatro principios cuando se está manipulando evidencia digital, los cuales se resumen a continuación:

- ✓ Ninguna acción realizada por los entes judiciales o sus agentes debe cambiar los datos almacenados en una computadora o en un medio de almacenamiento alterno debido a que ésta acción puede tener consecuencias en los tribunales.
- ✓ En circunstancias excepcionales, cuando una persona encuentra necesario acceder a los datos originales almacenados en una computadora o en un medio de almacenamiento alterno, dicha persona debe ser competente en ello y debe poder proporcionar una explicación de la relevancia e implicaciones de sus actos.
- ✓ Un registro de auditoría o cualquier otro registro que almacene todos los procesos aplicados a la evidencia digital debe ser creado y preservado. Una

tercera parte independiente debe ser capaz de examinar dichos procesos y llegar al mismo resultado.

- ✓ La persona a cargo de la investigación (el oficial del caso) tiene la totalidad de la responsabilidad en cuanto al aseguramiento del cumplimiento de las leyes y los principios dados desde el principio del proceso.

Por otro lado, The Proposed Standards for the Exchange of Digital Evidence [IOCE] sugiere un conjunto similar de principios para la estandarización de la recolección de evidencia digital:

- ✓ Tras la incautación de evidencias digitales, las acciones efectuadas sobre éstas no deben cambiarlas.
- ✓ Cuando sea necesario que una persona deba acceder a la evidencia digital original, dicha persona debe ser competente en dicho procedimiento.
- ✓ Toda la actividad relacionada con la incautación, acceso, almacenamiento o transferencia de evidencia digital debe estar documentada, preservada y disponible para futuras revisiones.
- ✓ Cualquier agencia que sea responsable de incautar, acceder, almacenar o trasferir evidencia digital es responsable del cumplimiento de éstos principios establecidos.

Los anteriores principios apuntan principalmente a asegurar la integridad y, por ende, admisibilidad de la evidencia digital durante todo su ciclo de vida.

The Electronic Crime Scene Investigation - A Guide for First Responders, propuesto por el departamento de Justicia de Estados Unidos, ofrece los siguientes lineamientos cuando se manipula evidencia digital:

- ✓ **Asegurar y evaluar la escena:** Se deben llevar a cabo una serie de pasos para asegurar la integridad de la evidencia potencial.
- ✓ **Documentar la escena:** Se debe crear un registro permanente de la escena, documentando tanto evidencia digital como evidencia convencional.
- ✓ **Recolección de evidencia:** Se debe recolectar tanto la evidencia tradicional como la digital de manera que se conserve el valor de dicha evidencia.

- ✓ **Empaque, transporte y almacenamiento:** Se deben tomar las precauciones adecuadas cuando se empaque, transporte y almacene la evidencia, manteniendo la cadena de custodia.

Por otro lado se encuentra una metodología de respuesta a incidentes la cual propone las siguientes fases cuando se produce un incidente o cuando se desea realizar una investigación digital:

- ✓ **Preparación pre-incidente:** Se realiza a través de entrenamiento y educación del personal, obteniendo conocimiento en cómo responder a incidente.
- ✓ **Detección de incidentes:** Se realiza desarrollando técnicas centradas en cómo detectar actividades sospechosas.
- ✓ **Respuesta inicial:** Consiste en confirmar que un incidente ha ocurrido y en obtener la evidencia volátil.
- ✓ **Formulación de la estrategia de respuesta:** Consiste en responder al incidente basándose en un conocimiento previamente adquirido concerniente a todos los hechos conocidos recolectados en la fase de respuesta inicial.
- ✓ **Implementación de las medidas de seguridad:** Consiste en aplicar las debidas medidas de seguridad para aislar los sistemas infectados.
- ✓ **Monitoreo de red:** En esta fase se monitorea el tráfico de red que sale o ataques adicionales que pueden ocurrir.
- ✓ **Recuperación:** Consiste en restaurar el sistema afectado para asegurar su estado operativo y que vuelva a funcionar correctamente.

Para finalizar, se expone a continuación las prácticas establecidas en el HB171:2003 Handbook Guidelines for the management of IT evidence desarrollado en Australia y explicado detalladamente en el documento “Buenas prácticas en la administración de la evidencia digital”.

Dicho documento “es un compendio de prácticas internacionales en el tema de evidencia digital disponibles a la fecha, que busca ofrecer un conjunto de elementos teóricos y prácticos para apoyar procesos donde este tipo de evidencia es fundamental

para avanzar en la solución de un caso” . El ciclo de vida para la administración de evidencia digital consta de seis pasos a saber:



Figura 2. 1. Ciclo de vida para la administración de evidencia digital

Fuente: Buenas prácticas en la administración de la evidencia digital”.

A continuación de enumeran las seis fases del ciclo de vida y se proporciona una pequeña descripción de cada una:

- ✓ **Diseño de la evidencia**: El objetivo principal de ésta fase del procedimiento es fortalecer la admisibilidad y relevancia de la evidencia producida por las tecnologías de la información proporcionando, por ejemplo, fechas y hora de creación o alteración, validación de autenticidad de los registros entre otras prácticas asociadas.
- ✓ **Producción de la evidencia:** El objetivo de ésta fase consiste en producir la mayor cantidad de información posible con el fin de aumentar las probabilidades de obtener e identificar la mayor cantidad de potencial evidencia digital relacionada con el incidente. Para realizar esto es necesario que el sistema computacional genere registros electrónicos, que se pueda

identificar el autor de dichos registros y que se pueda identificar la fecha y hora de creación de los registros entre otros.

- ✓ **Recolección de la evidencia**: El objetivo de ésta fase es localizar toda la evidencia digital y asegurar que todos los registros electrónicos originales no han sido alterados. Esta fase se relaciona con la primera parte de esta sección la cual habla de los principios que se deben tener en cuenta para manipular evidencia digital.
- ✓ **Análisis de la evidencia**: Esta fase consiste en realizar el ensamble, análisis y articulación de los registros electrónicos para establecer los hechos de los eventos ocurridos en el contexto de la situación bajo análisis.
- ✓ **Reporte y presentación:** El objetivo de ésta fase consiste en generar toda la documentación concerniente a los hallazgos, resultados, actividades, cadena de custodia de la evidencia y, en general, de todo lo realizado en el proceso de investigación.
- ✓ **Determinar la relevancia de la evidencia:** Esta fase consiste en valorar las evidencias de tal manera que se identifiquen las mejores evidencias que permitan presentar de una manera clara y eficaz los elementos que destaquen y se deseen presentar en el proceso judicial correspondiente.

Luego de realizar una revisión de algunos de los estándares y procedimientos más aceptados en cuanto a informática forense se refiere, se procede a continuación a proponer una guía metodológica para realizar análisis forenses orientados a incidentes en dispositivos móviles GSM, basado en los principios anteriormente descritos y aportando elementos que faciliten la obtención de evidencia digital relacionada con los detalles de un incidente ocurrido en un teléfono celular GSM.

2.10. Tecnología GSM

2.10.1. Contexto histórico de la tecnología

En los años 80, la industria de teléfonos móviles en Europa comenzó a presentar un crecimiento importante respecto a años anteriores, lo cual trajo como consecuencia colateral la aparición de diferentes estándares en esta industria por parte de diferentes

fabricantes. Estos sucesos, como se ha visto en la historia con otras tecnologías de alta relevancia, plantearon la necesidad de crear una unificación de tecnologías, para así generar una especificación estándar sobre la cual se pudiera trabajar de manera conjunta y beneficiosa.

"Así fue como inicio en 1982 el desarrollo del estándar GSM , en el cual participaron varios países europeos, los cuales serian los primeros beneficiados con la creación de esta especificación. Algunos años después, dado el éxito que tuvo el estándar, éste fue incluido en la ETSI (European Telecommunication Standards Institute, por sus siglas en ingles) lo cual prácticamente esparció el sistema en toda Europa, impulsando el desarrollo del estándar y la posterior finalización de la primera especificación.

La tecnología GSM, entre otras cosas, permitió tener un sistema de interconexión de redes locales e internacionales, manteniendo una identidad única en cualquiera de las locaciones en donde se encontrara un usuario gracias al sistema de roaming. Otra de las características importantes fue que el sistema era totalmente digital, a diferencia de los otros sistemas de telefonía móvil de la época, lo cual permitía manejar eficientemente tanto datos como voz sobre la misma red ."(Syngvar, 1994 :112).

Como dato concluyente, aunque existen mejores tecnologías desarrolladas desde ese entonces, hoy en día GSM es el sistema más utilizado alrededor del mundo, lo cual es clave para la investigación, sus fines y alcances.

2.10.2. Infraestructura del sistema GSM

El sistema GSM al igual que otros sistemas de telefonía móvil celular, está compuesta de manera modular de acuerdo con las especificaciones del estándar. Estos módulos o entidades, se encuentran conectados entre sí a través de interfaces propias. La infraestructura está dada por:

- **La estación móvil:** Este componente de la infraestructura es aquel que llega al usuario final, y se refiere al teléfono móvil, el cual se compone del aparato como tal, y la SIM Card, la cual identifica a ese aparato dentro de la red en que se encuentre presente, además de poseer más información relevante. A través de la

SIM Card se realiza la comunicación dentro de la red y entre diferentes redes locales e internacionales, por lo cual un teléfono para GSM no puede realizar ni transmisión de voz ni de datos sin tener una SIM Card asociada.

• **Estación de transmisión base:** Son antenas de recepción y envió de señales las cuales trabajan sobre una misma frecuencia dada por el proveedor de servicios.

Cada estación se encarga de ya sea enviar a una estación central datos y/o voz, o también de hacer el proceso inverso hacia una o varias estaciones móviles. (The Forensic Toolkit. Foundstone Network Security).

Estación controladora base: Como su nombre lo indica, esta estación se encarga de controlar varias estaciones de transmisión base, y también de varios procedimientos de configuración y parámetros de conexión, así como de enrutamiento de datos y voz hacia al respectivo centro de conmutación móvil.

• **Centro de conmutación móvil:** La función principal de este componente de la infraestructura GSM consiste en conmutar, ya sea voz o datos, entre estaciones controladoras base, estaciones de transmisión base, redes exteriores de telefonía móvil y fija.

• **Registros de localización:** Básicamente se manejan dos registros en este componente, el primero es el registro de localización de visitantes, y el segundo es el registro de localización local. El primer registro se encarga de manejar y almacenar los datos de estaciones móviles que no sean propiamente miembros de la red que opera en determinada área y están conectadas a través de roaming. Éste se encuentra asociado con uno o más centros de conmutación móvil. El segundo registro es el local, el del proveedor, y es en donde se tiene la información de los servicios que cada estación móvil tiene habilitados, registro de actividades por parte de cada estación móvil, localización, etc. Esta información también se encuentra disponible en el registro de visitantes.

• **Registro de identidad de equipos:** Este componente de la infraestructura es opcional y se encarga de registrar las estaciones móviles por parte del proveedor

con el fin de denegar servicios a aquellas otras estaciones que no se encuentren en este registro, ya sea porque pertenecen a otro proveedor o porque se encuentren reportadas como robadas o manipuladas.

2.10.3. Subscriber Identity Module – SIM Card

La SIM Card es un componente vital de la estación móvil, componente final de la infraestructura (MAlies, S García, F Molina, J Montoya, M Serrano. "Técnicas forenses en Medios Inalámbricos"). Éste componente identifica a un usuario único dentro de una red de teléfonos GMS y también posee información independiente a la del teléfono. Entre la información más importante que se almacena en este módulo esta: (Casadei, A Savoldi, P Gubian : 120)

• **Información acerca del subscriptor:** IMSI (identificador único para cada subscriptor en el sistema), información sobre lenguajes preferidos, Mobile Station

ISDN (MSISDN) el cual puede ser usado para recuperar las llamadas originadas por el usuario a otros números de teléfono.

• **Información sobre los conocidos del suscriptor:** Los suscriptores pueden mantener una lista de números a los cuales llama o de los cuales es llamado, y dependiendo del número de llamadas se puede deducir la importancia de dicho contacto en la investigación.

• **Información sobre el tráfico SMS:** Es posible leer mensajes enviados y recibidos por el subscriptor fuera de la SIM card y saber por cada mensaje si fue leído o no.

• **Información sobre la localización del suscriptor:** La SIM guarda la última área en donde el suscriptor se registró ante el sistema.

• **Información sobre llamadas:** Los últimos números marcados son guardados en un archivo en el filesystem de la SIM. La llave usada para cifrar la última llamada también es guardada allí.

• **Información sobre el proveedor:** Es posible obtener el nombre del proveedor y la red celular comúnmente usada para la comunicación, junto con las redes que están prohibidas para el suscriptor.

• **Información sobre el sistema:** Cada SIM card tiene un único ID almacenado. Todos los servicios que el suscriptor pueda tener activados, dependiendo del estado actual de habilitación, pueden estar almacenados en la SIM

Esta información es relevante a la hora de realizar una investigación forense que implique un teléfono GSM, debido a que éste es el principal banco de información primaria del equipo. Dada su importancia respecto a la riqueza de datos que presenta una SIM Card, esta tiene sus propios mecanismos de validación de usuarios y seguridad, los cuales son: (Smith:85).

• **PIN (Personal Identification Number):** Al intentar acceder la información de la SIM Card o a sus servicios, en primera instancia se requiere ingresar el número de identificación personal de la tarjeta. En caso de que sea ingresado erróneamente determinado número de veces, automáticamente la SIM Card se bloquea para el acceso a través del ingreso del PIN, siendo necesario el acceso a través del ingreso del código PUK, suministrado como llave única de la tarjeta por el fabricante o el proveedor.

• **PUK (Personal Unlock Code):** Este código sirve para habilitar la SIM Card debido al acceso incorrecto del PIN. Este código es proporcionado ya sea por el fabricante o por el proveedor de servicios. Si el PUK es ingresado de manera incorrecta determinado número de veces, la información de la SIM Card se eliminara de manera automática y de manera irrecuperable, protegiendo así la información de personal no autorizado al acceso a ésta.

2.10.4. Entendiendo los dispositivos móviles

Para entender con mayor detalle los problemas y amenazas a las cuales están expuestos los teléfonos celulares, es necesario conocer de forma general las características y funcionalidades de éstos para así lograr obtener los conocimientos

necesarios para diseñar una metodología de recolección de evidencia digital en dispositivos móviles (celulares GSM).

En el mercado existe gran variedad de dispositivos que encajan fácilmente en la categoría de dispositivos móviles, sin embargo, dado que el enfoque de la investigación en curso está dirigido a los teléfonos móviles GSM, sólo se presentará una breve reseña de dispositivos como BlackBerrys, Pocket PC y Palm Handheld, y posteriormente se hará énfasis en teléfonos móviles, en especial en aquellos que cuentan con el sistema operativo Symbian.

2.10.4.1. BlackBerrys

"Los BlackBerrys inicialmente fueron una solución que se dio a la necesidad de interconexión entre personal de empresas para el uso de mensajes instantáneos, voz, e-mail, agenda de contactos, etc., de manera instantánea a través del uso de redes inalámbricas y la característica de portabilidad del dispositivo" (Swenson, G Manes and S Shenoi, "Imaging and Analysis of GSM SIM cards").

Al pasar de los años, las funcionalidades de estos dispositivos fueron aumentando gracias a los avances tecnológicos crecientes, añadiendo funcionalidades como mapas, GPS, organizador, aplicaciones, juegos, cámara integrada, etc. (Casadei, A Savoldi, P Gubian, "Forensics and SIM cards: an Overview").

Hoy en día, existen dos categorías en las cuales los BlackBerrys están presentes dadas las necesidades del mercado. La primera de ellas va dirigida a las personas del común, presentando para ellos dispositivos compactos y limitados. La segunda categoría va dirigida a los negocios, presentando dispositivos más avanzados, para suplir necesidades puntuales.

Entre las características que estos dispositivos tienen en sus diferentes modelos, se encuentran: (BlackBerry. "What is Blackberry)

- Bluetooth
- Media player, MP3/AAC/MPEG4/

• Ranura de expansión de memoria MicroSD

• Pantallas de alta resolución

• Soporte para redes GSM/GPRS y redes EDGE

• Soporte para redes wireless RIM

2..10.4.2. Pocket PCs

Estos dispositivos fueron concebidos por empresas como Compaq, HP, entre otros, para suplir necesidades de organización, agenda, conexión inalámbrica redes, correo, y demás funcionalidades estándar de una PDA.

"Una de las características principales de estos dispositivos, es el uso de uno de los sistemas operativos populares en esta rama de PDA's, como lo es Windows Mobile, y por ende, la arquitectura particular que esto conlleva. Esta arquitectura, se ve muy marcada en la manera en que estos dispositivos manejan la memoria para realizar la persistencia de sus datos, priorizando los archivos de su propio sistema, así como su registro, y beneficiando al usuario al brindarle en la mayoría de sus modelos mecanismos de memoria no-volátil para el guardado de datos." (The Forensic Toolkit. Foundstone Network Security:96).

Entre las características de hardware que estos dispositivos manejan se encuentran:

• Bluetooth

• Reproducción de contenido multimedia

• Ranura de expansión de memoria SD

Pantallas de alta resolución

• Soporte para redes GSM/GPRS en dispositivos con teléfono integrado.

• Soporte de Wi-Fi en sus diferentes estándares.

2.10.4.3. Palm Handhelds

Al igual que las Pocket PC, las Palm Handhelds son dispositivos portátiles que ofrecen servicios de información a personas y empresas de manera portátil, dadas sus características de conectividad y estación móvil de trabajo.

Existen dos diferencias que valen la pena resaltar entre las Palm Handhelds y las Pocket PC. La primera de estas es el sistema operativo, el cual inicialmente fue Palm OS, el cual maneja un único formato de archivos, limitando la interacción con cualquier otro tipo de dispositivo diferente de una Palm. La segunda diferencia se encuentra en el manejo de la memoria, ya que los dispositivos Palm almacenan los datos del usuario en memoria volátil, lo cual significa que dada una pérdida de energía total en el dispositivo, los datos del usuario desaparecen.

Sin embargo, esto último ha venido cambiando en algunos productos que ofrece Palm, como su modelo Tungsten TX, el cual maneja memoria no-volátil para los datos del usuario, así como gran parte de la serie Treo, también de Palm, la cual ha migrado al sistema operativo Windows Mobile, que brinda un mejor soporte para comunicaciones celulares que el que da Palm OS.

2.11. Teléfonos celulares

2.11.1. Funcionalidades

Los teléfonos celulares tienen las mismas funcionalidades de un teléfono estándar, con la ventaja de comunicarse a través de ondas de radio entre estaciones base. Esto permite la transmisión de voz. Sin embargo, en la actualidad, estas funcionalidades se han extendido, permitiendo a los teléfonos transmitir a parte de voz, elementos de datos, como SMS, imágenes, video, archivos enteros, etc.

2.11.2. Hardware

Las características de hardware a destacar son las siguientes:

- Los teléfonos móviles están compuestos por un microprocesador, una memoria de solo lectura (ROM), una memoria de acceso aleatorio (RAM), un modulo

de radio, un procesador de señales digitales, un micrófono y un parlante, un teclado y una pantalla de cristal liquido (LCD).

- El sistema operativo del dispositivo se encuentra en la ROM la cual puede ser borrada y re programada electrónicamente con las herramientas apropiadas.
- La RAM, la cual es usada para guardar datos del usuario, es soportada por la batería. Si la batería falla, la información se puede perder.
- Los dispositivos más recientes están equipados con varios microprocesadores en niveles que reducen el número de chips requeridos para operar el teléfono e incluyen una capacidad de memoria considerable. Otras nuevas funcionalidades que tienen es que soportan slots de memorias extraíbles o periféricos especializados tales como wireless (Esta tecnología está construida dentro del teléfono).
- Los teléfonos móviles pueden ser clasificados de la siguiente manera: Teléfonos básicos los cuales tienen funcionalidades simples como comunicación por voz y mensajes de texto, teléfonos avanzados los cuales tienen funcionalidades adicionales de multimedia y los Smarth Phones los cuales combinan las capacidades de los teléfonos avanzados con los PDA. (S. Radack : 385).

2.11.3. Teléfonos con Sistema Operativo Symbian

Como se mencionó previamente en el documento, la intención es darle cabida a una sección en donde se hable del sistema operativo Symbian, diseñado para teléfonos móviles, el cual es uno de los principales sistemas operativos para este tipo de teléfonos. A continuación veremos algunas características del sistema operativo, y algunos fabricantes con sus respectivas series de teléfonos que soportan Symbian.

2.12. El Sistema Operativo Symbian

Symbian OS, es el principal y más avanzado sistema operativo en industria de teléfonos móviles de última generación. Fue diseñado para cumplir con los requerimientos de teléfonos que soportan tecnología 2.5G y 3G.

Con gran variedad de funcionalidades, es un sistema que brinda un buen nivel de desempeño, en procesamiento, multimedia, servicios para aplicaciones y genéricas del sistema, comunicaciones, y lo más importante, de seguridad.

Es importante resaltar este último elemento, el de seguridad, debido a la vital importancia que tiene para la investigación el poder trabajar con un sistema operativo que brinde ciertas facilidades y niveles de confianza a la hora de realizar un análisis forense. Entre las características de seguridad se encuentran: (Symbian. "Symbian OS 9.5").

- Encapsulamiento de datos por parte de las aplicaciones
- Uso de algoritmos criptográficos, como DES, 3DES, RC2, RC4, RC5 y AES.
- Soporte para IPSec y clientes VPN.
- Limitaciones según permisos de usuario
- Persistencia de datos a través de una base de datos SQL embebida.
- Soporte de MIDP 2.0 (Mobile Information Device Profile, por sus siglas en ingles)
- Uso de protocolos seguros, como HTTPS, SSL y TLS
- Capacidad de monitoreo por aplicación.

2.13. Modelos de Memoria

2.13.1. Procesos: En Symbian, los procesos son instancias sencillas de archivos ejecutables, las cuales pueden o no generar hilos de proceso, los cuales algunas veces comparten información entre ellos; esto dependiendo del modelo de memoria que el diseñador de los ejecutables haya establecido. Idealmente lo mejor es no permitir que estos procesos interfieran con otros, con excepción de los procesos locales del sistema.

"El funcionamiento básico de la creación de procesos, se encuentra dado por un cargador de procesos, el cual crea un objeto de tipo DProcess, comando con el cual se

carga el proceso, y se le informa al kernel del sistema que esta acción fue realizada. El kernel por su lado, abre un nuevo hilo para este proceso, y lo marca como hilo principal de dicho proceso, a través del comando KThreadFlagProcessPermanent ” (J Sales, 2005: 381).

Como los procesos en un sistema operativo de escritorio, estos tienen ciertas características importantes a citar:

- Uso de prioridades por parte de los procesos.
- Cuando un proceso padre de otros procesos es terminado, todos sus procesos dependientes, también son terminados.
- Hilos del mismo proceso pueden compartir objetos. Para buenas prácticas de programación, esto no debería ser posible para diferentes procesos.
- Un usuario, solo puede crear un nuevo hilo dentro de su propio proceso.

2.13.2. Listado de procesos del sistema: Es importante citar los procesos del sistema, especialmente los procesos que se cargan cuando el sistema inicia y queda en stand-by esperando a ser utilizado. El esquema de carga esta dado de la siguiente manera:

• Bootstrap

• Kernel, Variantes y Extensiones del mismo

• Servidor de Archivos y Sistema de Archivos

• Arranque del sistema

• GUI y otros procesos secundarios

Se explicaran a fondo los 3 primeros puntos del esquema de carga, debido a que los 2 últimos puntos se refieren a un punto de alto nivel, en el cual por el momento no se enfocará la investigación.

2.14. La tecnología GSM y los problemas de seguridad en dispositivos móviles

Un teléfono ya no es más un teléfono y un BlackBerry ya no es más un BlackBerry. Todos estos dispositivos deben ser considerados ahora como "Estaciones de trabajo empresariales móviles". Estos dispositivos son abundantes en cualquier lugar, se encuentran en aeropuertos, restaurantes, centros comerciales etc. Cada vez más personas los utilizan, entre ellas empresarios los cuales, gracias a dichos aparatos, pueden mantenerse en contacto con su negocio. Desde luego esto es de gran valor para las empresas ya que permiten el trabajo desde casi cualquier lugar, sin embargo, surge un inconveniente.

A pesar de que estos dispositivos son, a su vez, teléfonos celulares, en el fondo son realmente computadoras móviles las cuales contienen información corporativa sensible la cual puede ser guardada fácilmente en un bolsillo. Esto, sumado a que la comunicación de estos aparatos es esencialmente inalámbrica, plantea un gran interrogante en cuanto a seguridad de la información se refiere. Finalmente, las computadoras móviles (como las BlackBerry y los celulares) nunca reciben las mismas consideraciones de seguridad que las computadoras tradicionales.

Debido a las funcionalidades que tienen hoy en día los llamados "dispositivos móviles", ya no se pueden clasificar como teléfonos celulares o asistentes personales sino que son una mezcla de éstos y por esto, al igual que sus semejantes los computadores de escritorio, necesitan ser protegidos de las amenazas que actualmente atentan contra la información.

Primero se realiza una revisión de la tecnología GSM, de la cual hacen uso los dispositivos para los cuales va a ser diseñada la metodología. En dicha revisión se expondrá el contexto histórico de la tecnología, la infraestructura del sistema GSM en donde se explica el funcionamiento de la tecnología y finalmente el elemento de hardware principal de los dispositivos GSM: La SIM card.

Finalmente se realiza una revisión de los "problemas de seguridad de los teléfonos celulares GSM en donde se utiliza la clasificación de los problemas de seguridad sugerida por Hoffman en la cual se sugieren las siguientes categorías de clasificación:

Malware, ataque directo, interceptación de la comunicación y autentificación, spoofing y sniffing". (D Hoffman. "Blackjacking": 121).

Kernel,variantes y extensiones: El kernel del sistema, realiza toda su ejecución de manera secuencial, ejecutando rutinas de inicialización, denominadas init-0 a init-3. Aquí se cargan todos los servicios primitivos del sistema, acorde con la especificación del teléfono. Init-0 comienza justo después de la ejecución de EKERN.EXE:KernelMain().

• Init-0: Desde el KernelMain(), el hilo inicial invoca el siguiente comando P::Create-Variant(), el cual realiza toda la creación de variantes concerniente a init-0. Una vez creadas las variantes necesarias, se invoca el procedimiento Initialise(), en donde se exportan las variantes creadas, y se da paso a init-1.

• Init-1: Una vez realizadas las tareas de init-0, el siguiente paso es la ejecución del microkernel, a través de la llamada del constructor K::InitialiseMicrokernel(). Esto da paso a la ejecución de los siguientes componentes:

a. Memory Management Unit (MMU) y el administrador de la memoria caché

b. Administrador del co-procesador

c. Despachadores de interrupciones

d. Servicios de información, Almacenamiento y Recuperación

e. Modos de excepción para modos IRQ, FIQ, ABT y UND

Cuando se realiza la carga de estos componentes, el kernel genera un espacio en memoria, que está reservado para el bootstrap, el cual es fijo por el momento. También, el kernel ya está habilitado para la creación dinámica de objetos:

a. El kernel inicializa los datos locales en sus valores por defecto
b. El kernel crea un objeto de tipo DProcess, el cual representa el proceso EKERN

c. El kernel crea un hilo de tipo DThread, el cual representa la instancia de ejecución actual, que al final quedara con un valor null o idle.
d. El kernel desbloquea el planificador del sistema

• Init-2: Con los servicios anteriormente iniciados, el kernel procede a completar la inicialización del administrador de memoria. Aquí se crean todas las regiones de memoria virtual y se recuperan datos que puede que hayan persistido después de un reinicio del sistema.

El resto de funciones que se cargan en esta etapa son:

a. Los contenedores de objetos son creados, y los procesos iníciales e hilos se adjuntan a ellos.
b. El kernel activa todas las capacidades de utilización de la RAM
c. La interfaz del debugger se inicializa
d. Los servicios Publish y Subscribe se inicializan
e. Los perfiles de energía se inicializan

• Init-3: Finalmente, en la última etapa de inicialización del kernel, se realiza la carga de los siguientes servicios: (S.Ismail y Z Yunos. "Worms and Trojans go mobile)

a. Carga del HAL13 System del lado del kernel
b. Creación de la cola de eventos
c. Colas DFC14 por defecto
d. El sistema de reloj, y reloj secundario el sistema

2.15. Problemas de seguridad en teléfonos celulares GSM

"Los teléfonos celulares actualmente tienen una gran variedad de funcionalidades: Pueden tomar fotos, grabar videos, reproducir música; tienen acceso a datos de forma inalámbrica e incluso tienen calendarios y agenda de contactos las cuales se pueden sincronizar inalámbricamente con un computador de escritorio. La mayoría de personas en la actualidad tienen un dispositivo de este tipo; sin embargo, numerosos virus han venido apareciendo especialmente para infectar teléfonos móviles. Estos se

han venido convirtiendo en el objetivo preferido por los atacantes debido a las vulnerabilidades y a la poca protección que tienen" (B. Rayner. "Mobile Phone Security").

Sin embargo, los dispositivos móviles no están expuestos solamente a ataques de "código malicioso", existen otros tipos de amenazas como son los ataques directos, la intercepción de la comunicación, los ataques de autentificación y los incidentes a las instalaciones físicas. Para realmente entender cómo realizar análisis forenses orientados a incidentes en un dispositivo GSM, es necesario entender algunos tipos de amenazas para poder concebir dónde y cómo se almacena la información que puede potencialmente puede contener evidencias digitales para el análisis forense.

Considerando lo expuesto, se utilizará el sistema de clasificación de vulnerabilidades en dispositivos móviles propuesto por Hoffman. Hoffman clasifica las diferentes fallas de seguridad identificadas en dispositivos móviles en las siguientes categorías definidas: código malicioso, ataques directos, intercepción de la comunicación, ataques de autenticación y los incidentes en las instalaciones físicas.

2.15.1. Malware

El malware es la amenaza de seguridad mejor conocida actualmente debido a que incluso los usuarios casuales de éstos dispositivos saben algo sobre los virus y entienden que un programa antivirus es necesario para proteger el computador de los virus. "El malware es una porción adicional de datos, llamado código malicioso, el cual es adherido a un programa. En el momento en que el usuario ejecuta dicho programa, automáticamente se carga el código adicional, infectando el computador con el virus. Los ataques pueden venir vía Bluetooth, programas maliciosos de Internet." (D. Hoffman, 2007: 185).



Figura 2. 2.Formas de Ataque del malware

Fuente: D. Hoffman

"Symbian OS es el sistema operativo licenciado utilizado por los mayores fabricantes de teléfonos celulares en el mundo como Nokia, Motorola y Sony Ericsson. Algunos de los smart phones que utilizan Symbian son el Nokia 6600, el Sony Ericsson P900 y el Motorola A925. Estos teléfonos, así como los computadores de escritorio, son vulnerables a amenazas de seguridad tales como troyanos y gusanos"(S. Ismail y Z Yunos, 2005: http://www.cybersecurity.org.my/data/content_files/13/91.pdf?.diff=1176416843), los cuales son tipos de malware bien conocidos.

Las amenazas no solo conciernen a los dispositivos móviles sino que algunos de estos virus se pueden infiltrar en una conexión Wi-Fi esparciéndose del teléfono celular a servidores, computadores de escritorio y computadores portátiles, contaminando información importante (B. Rayner. "Mobile Phone Security". East Carolina University).

"El gusano Cabir fue la primera pieza notable de malware para teléfonos celulares. Este virus está dirigido a dispositivos que tienen el sistema operativo Symbian, entre ellos la serie 60 de Nokia y, en especial, su interfaz de usuario. Una vez el dispositivo se encuentra infectado con el virus, Cabir usa la tecnología Bluetooth para auto-enviarse a todos los contactos de la agenda del teléfono celular. El virus se presentaba

así mismo ante los usuarios como “Caribe Security Manager” y se instala mediante el archivo CARIBE.SIS”.

(http://www.infosecwriters.com/text_resources/pdf/Phones_BRayner.pdf)

“Al momento de la infección, al ejecutar el archivo de instalación, la pantalla del teléfono celular muestra la palabra “Caribe”. Además de esto, el gusano modifica el sistema operativo Symbian del teléfono para que Cabir sea lanzado cada vez que el teléfono celular sea encendido. Luego de realizar la búsqueda de objetivos a infectar mediante Bluetooth, el teléfono envía el archivo “Velasco.sis” el cual contiene el gusano listo para instalar”

(http://www.cybersecurity.org.mx/data/content_files/13/91.pdf?.diff=1 176416843).



Figura N ° 2.2. Mensaje de Infección

Fuente: B. Rayner

“Cabir se replica sobre Bluetooth en el archivo caribe.sis que contiene el ejecutable principal del gusano caribe.app, el de reconocimiento del sistema flo.mdl y el archivo de recursos caribe.rsc.” (K.Saavedra. “Nuevo gusano que corre en teléfonos celulares que utilizan Symbian”. Microasist.

http://microasist.com.mx/noticias/nv/ksonv150604.shtml). Cuando el archivo caribe.sis se instala se copia los ejecutables del gusano en las siguientes ubicaciones:

c:\system\apps\caribe\caribe.rsc

c:\system\apps\caribe\caribe.app

c:\system\apps\caribe\flo.mdl

Cuando el archivo caribe.app se ejecuta, copia los siguientes archivos:

flo.mdl a c:\system\recogs

caribe.app a c:\system\symbiansecuredata\caribesecuritymanager\

caribe.rsc a c:\system\symbiansecuredata\caribesecuritymanager\

"Esto no sucede cuando la aplicación se instala en la tarjeta de memoria. Investigadores de F-Secure creen que el autor de Cabir liberó el código fuente del gusano en Internet y, debido a esto, se han encontrado dos nuevas versiones: Cabir.H y Cabir.I. Estas dos nuevas variantes no destruyen datos en los teléfonos que infectan, sin embargo, bloquean las conexiones Bluetooth legítimas y consumen rápidamente la batería del teléfono celular" (S. Ismail y Z Yunos. "Worms and Trojans go mobile". National ICT Security and Emergency Response Centre. 2005).

"Otro malware conocido es RexSpy, el cual puede ser diseminado enviando un mensaje SMS invisible al usuario. Este mensaje facilitaría el espionaje del teléfono celular infectado. Algunas características del malware son" (D.Hoffman , 2007: 198):

- Puede ser diseminado muy fácilmente.
- Puede ser diseminado de forma invisible.
- Permite a un hacker escuchar las conversaciones telefónicas.
- Permite a un hacker tener acceso completo a la agenda telefónica.
- Permite a un hacker acceder a todos los mensajes SMS.

"RexSpy, el rey del malware para teléfonos celulares, fue mostrado al público por la firma alemana SecurStar Gmbh como una demostración de las fallas de seguridad en los dispositivos móviles del momento y, por lo tanto, nunca fue diseminado masivamente, sin embargo, existen otras herramientas disponibles que tienen funcionalidades muy similares" (D.Hoffman , 2007: 199).

"FlexiSpy es un programa disponible para la compra, diseñado por una compañía Tailandesa llamada Vervata. Dicho software ha sido sujeto de una gran controversia

debido a las funcionalidades que tiene, entre las cuales se encuentran" (FlexiSpy. "FlexiSpy Features Compare".2008. http://www.flexispy.com/spyphone-features-compare.htm):

• Escucha de llamadas remota.

• Control del teléfono celular a través de mensajes SMS.

Almacenamiento de SMS y correos electrónicos enviados.

• Almacenamiento del historial de llamadas.

• Rastreo de la ubicación del teléfono.

• Interceptación de llamadas.

• Rastreo GPS.

• Notificación de cambio de SIM.

"Otro de los malware más conocidos es el troyano Skulls. El virus ha sido detectado en varios países incluyendo China, India, Turquía, Filipinas y Finlandia. Skulls deshabilita aplicaciones, instala gusanos Cabir e informa al usuario que ha sido infectado mostrando una serie de calaveras en el menú principal del dispositivo" (D.Hoffman , 2007: 201).

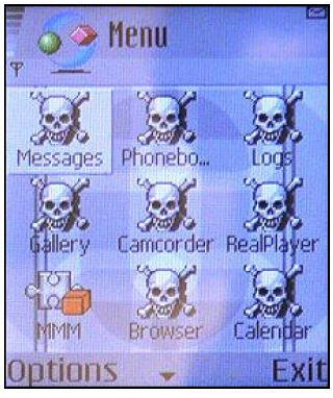


Figura 2. 3. Mensaje de Infección

Fuente: D. Hoffman

“El virus aparenta ser un manejador de temas para el teléfono, es decir, un archivo que le cambia la apariencia al teléfono celular colocando nuevos iconos, fondos de pantalla etc., sin embargo, Skulls lo que realiza en realidad es deshabilitar aplicaciones como la cámara o la funcionalidad de enviar mensajes de texto. Solamente permite las opciones de recibir y realizar llamadas. Además de esto, también se encarga de bloquear las conexiones normales de Bluetooth consumiendo rápidamente la batería del dispositivo al estar constantemente en búsqueda de conexiones para así poderse auto-enviar” (B. Rayner. “Mobile Phone Security”. East Carolina University. http://www.infosecwrite rs.com/text_resources/pdf/Phones_BRayner.pdf).

Las últimas versiones de este malware aparentan ser una nueva versión del programa Macromedia.

Capítulo III

MARCO REFERENCIAL

3.1. Descripción del Contexto

Desde hace algunos años, se ha presentado un crecimiento importante en la utilización de dispositivos móviles en la vida diaria dado que permiten portar datos personales de forma práctica, fácil y cómoda. Estos datos son, en muchos casos, objetivo de personas mal intencionadas, que aprovechando las vulnerabilidades que presentan este tipo de dispositivos, son capaces de hurtar y/o utilizar estos datos con fines ilegales.

El Instituto de Seguridad Informática CSI (Computer Security Institute) publica cada año un reporte llamado "CSI Computer Crime and Security Survey" en el cual se realiza un resumen y exposición de la situación actual de la seguridad informática y del crimen cibernético mostrando una serie de estadísticas basadas en hechos relacionados con seguridad de la información ocurridos en diferentes empresas a nivel mundial. A continuación se muestran una serie de gráficas las cuales proporcionan una visión actual de la seguridad informática y, por ende, de la necesidad de la informática forense en el mundo, las cuales sin embargo pueden tener cifras aun más elevadas debido a la gran cantidad de incidentes que no son detectados por los expertos de seguridad en las distintas compañías.

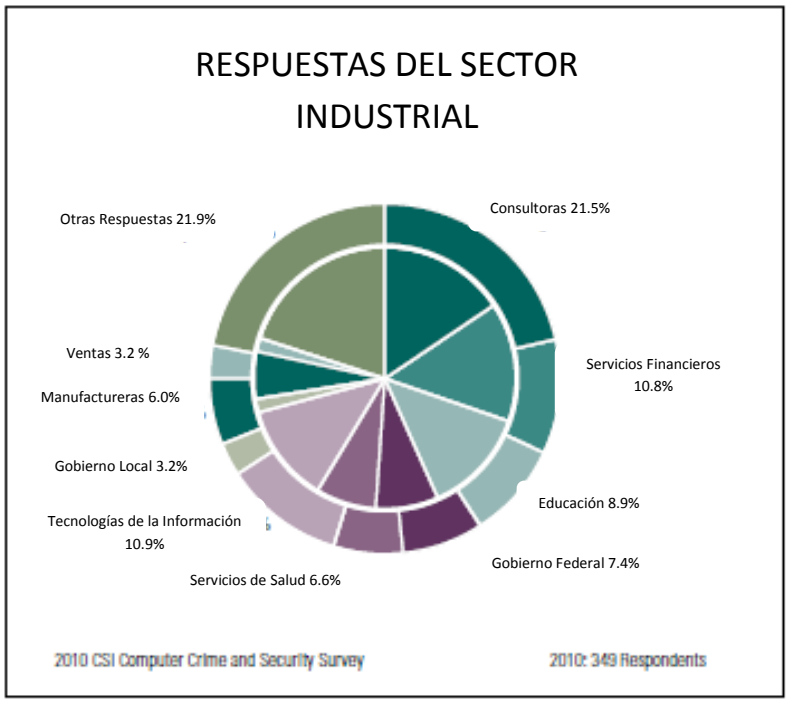


Figura 3. 1.Seguridad Informática (Respuestas del Sector Industrial)

Fuente: Instituto de Seguridad Informática

Traducción: Propia

En la grafica 3.1. se observa que muchas instituciones tanto del sector público como privado se han visto afectadas por el crimen cibernético, lo cual indica que el número de ataques al año es mucho mayor, lo que demuestra el estado crítico de la seguridad informática actualmente. Cabe señalar también que las instituciones financieras ya no están dispuestas a hablar de sus incidentes.

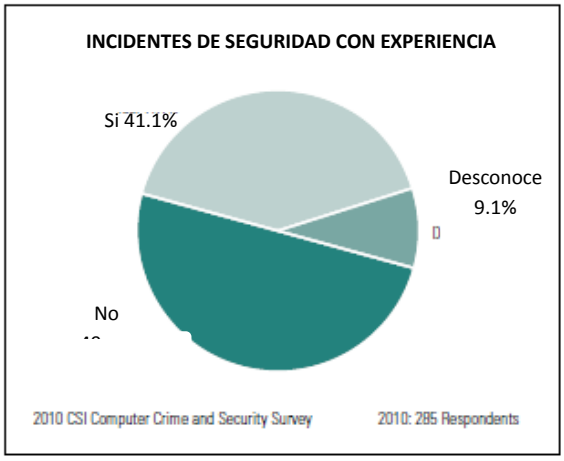


Figura 3. 2.Incidentes de Seguridad con Experiencia

Fuente: Instituto de Seguridad Informática

Traducción: Propia

La figura N°3.2. muestra que el 49,8% afirma que los incidentes de seguridad no son relevantes ya que no fueron amenazados; sin embargo el 41.1% señala que si se vieron amenazados, pero las amenazas son de muchos tipos y de una gama de posibles consecuencias.

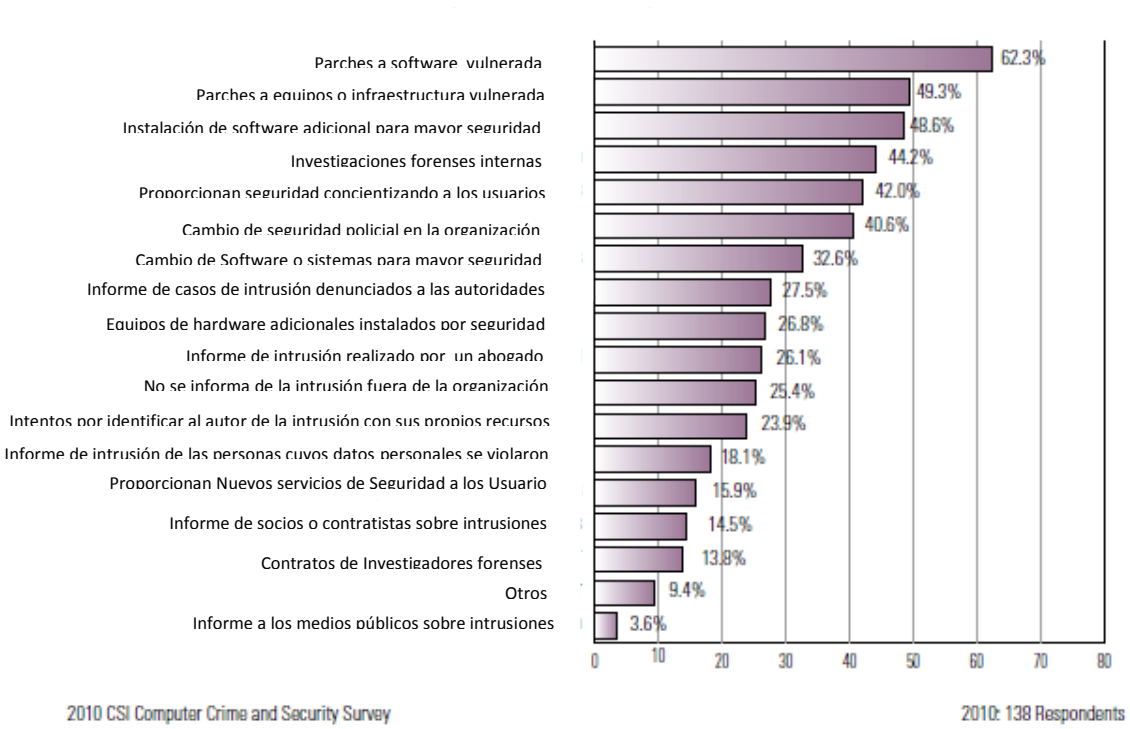


Figura 3. 3.Acciones realizadas después de un incidente

Fuente: Instituto de Seguridad Informática

Traducción: Propia

La figura 3.3. muestra , que el 62.3% de los encuestados realiza un parche al software vulnerado esto con el objetivo de superar sus vulnerabilidades.

El 44.2 % realiza actividades de investigación forense interna con el fin de detectar y establecer medidas para contrarrestar vulnerabilidades. Y solo 27.5% de los encuestados reportaron el incidente a las autoridades correspondientes.

Con estos datos se concluye que la informática forense es cada vez más utilizada y que se está convirtiendo en una disciplina fundamental en el mundo digital actual.

Por otro lado, el uso de teléfonos celulares en la actualidad es bastante alto alrededor del mundo.

Más del 70% de la población del mundo ahora tiene un teléfono móvil, que se descompone a más de 5 mil millones de abonados móviles en todo el mundo con los países más desarrollados muestran el uso de móviles en 9 de cada 10 personas. Una estadística más bien triste, pero cierto es que los niños son más propensos a poseer un teléfono móvil que un libro, con un 85% de los niños que tienen un teléfono en comparación con el 73% que poseen libros.

Otros datos muy interesantes muestran que más de mil millones de los 4 millones de usuarios de teléfono móvil están usando los teléfonos inteligentes o smartphones. 3.000 millones mensajes SMS se lanzan a diario. Se predice que para 2014 el uso de Internet móvil superará el uso de Internet escritorio.

País	Habitantes	Telefonía Celular: Porcentaje de penetración
Argentina	39.921.833	**63%**
Bolivia	9.627.269	**82%**
Brasil	188.000.000	**53%**
Colombia	42.090.502	**90%**
Costa Rica	4.300.000	**51%**
Chile	16.134.219	**87%**
México	103,000.026	**50%**
Uruguay	3.415.920	**37%**[4]
Venezuela	26,012,000	**89%**

Figura 3. 4.Penetración de la telefonía móvil en América Latina

Fuente: Consultora Argentina Latin

Según lo señala una encuesta elaborada por la consultora Argentina Latin Panel en 9 mil hogares de 16 ciudades principales en 15 países latinoamericanos, la telefonía móvil tiene una penetración del 90% en Colombia, seguido muy de cerca por Venezuela con el 89%, Chile con 87%, y Bolivia con 82%. Más abajo se ubican Argentina, con el 63% de penetración en este segmento; Costa Rica, con el 51%, y Honduras con el 49%.

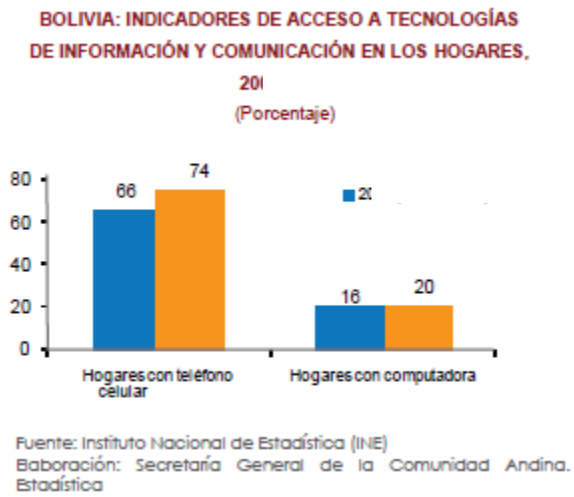


Figura 3. 5. Acceso a Tecnologías de Información en Bolivia

Fuente: Instituto Nacional de Estadística (INE)

En el año 2010, **Bolivia** registró que, el 74% de los hogares disponía de teléfono móvil, representando 8 puntos porcentuales más que lo observado en el año 2009 (66%). Con respecto a los hogares con computadora, también presentó un incremento de 4 puntos porcentuales.

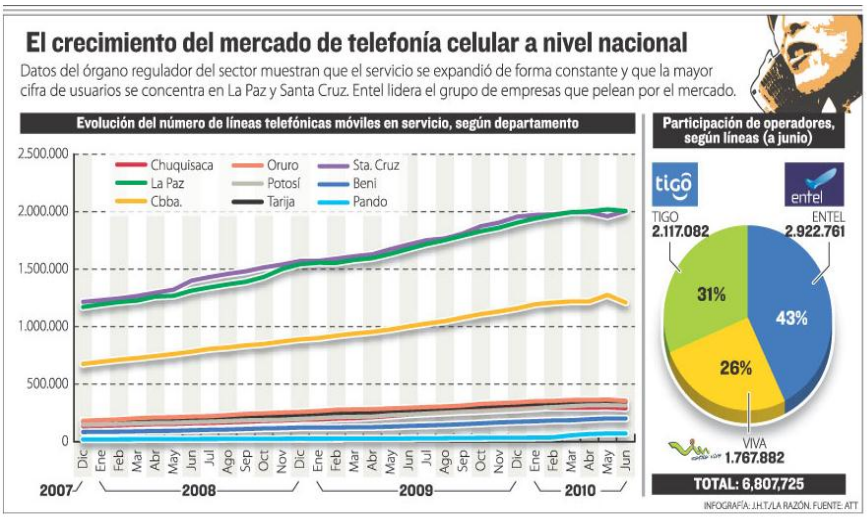


Figura 3. 6. Crecimiento del Mercado de Telefonía Celular en Bolivia

Fuente: Autoridad de Fiscalización y Control Social de Telecomunicaciones y Transportes (ATT)

De acuerdo a la figura 3.6. se puede observar que la telefonía móvil en el país creció de forma sostenida en los últimos 10 años. La penetración del servicio llega al 65%, es decir, por cada 100 habitantes hay 65 líneas celulares. Entre diciembre del 2009 y junio del 2010 la cantidad de usuarios se incrementó en 105,3%.

En 1996, cuando la telefonía móvil llegó al país, se contaba sólo con 33.400 líneas. datos de la Autoridad de Fiscalización y Control Social de Telecomunicaciones y Transportes (ATT) muestran que cuatro años después, el 2000, la cifra aumentó a 582.620.

Desde entonces, el crecimiento en el número de líneas móviles fue constante y superior al 100% cada año, según las estadísticas del órgano regulador. En diciembre del 2009, sumaban 6.464.390 y a junio del 2010 se incrementaron a 6.807.725 (105,3%).

Se precisó que Oruro tiene el índice más alto (81%), seguido de Santa Cruz (71%), La Paz (69%) y Tarija (66%).

De los párrafos anteriores se pude concluir que los teléfonos móviles están por todas partes y no sólo sirven para marcar números. Al aumentar su memoria y contar con herramientas de organización cada vez más complejas y cámaras de más calidad, su papel en la vida de casi todo el mundo incluidos los delincuentes va en aumento.

Traficantes de drogas, violadores y asesinos de varios países han sido atrapados en parte gracias a los artefactos electrónicos que llevan. Pero recabar pistas e indicios de la tecnología móvil no es fácil.

A diferencia de los ordenadores personales, que en un 90% de los casos o más utilizan el sistema operativo Windows, el funcionamiento de los móviles se basa en un confuso embrollo de programas que varía según el fabricante, incluso el teléfono. Con frecuencia, los datos están ocultos o codificados. Y, mientras un móvil esté conectado a su red celular, siempre habrá la posibilidad de que su historial de llamadas y sus mensajes de texto sean borrados, a propósito o no.

Basado en lo anterior, es importante seguir un procedimiento estándar que asegure la protección y el análisis exitoso de la evidencia digital con el fin de encontrar la mayor cantidad de detalles sobre el incidente ocurrido en el dispositivo, sin embargo, para diseñar una metodología es necesario revisar con detenimiento los procedimientos y estándares establecidos en la actualidad para considerar las mejores prácticas y fases expuestas, generando con ello un esquema metodológico que, sumado al aporte de análisis de incidentes, resulte la metodología propuesta.

3.2. Aplicación de Herramientas de Campo

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. Tenemos así, 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.

Entre las actividades más destacables en Bolivia, podemos citar el entrenamiento de funcionarios de varias instituciones: Banco Mercantil, Entel, FELCC, FELCN, Viceministerio anticorrupción, y otros.

Entre las actividades 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. (http://www.nobosti.com/spip.php?article539).

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.

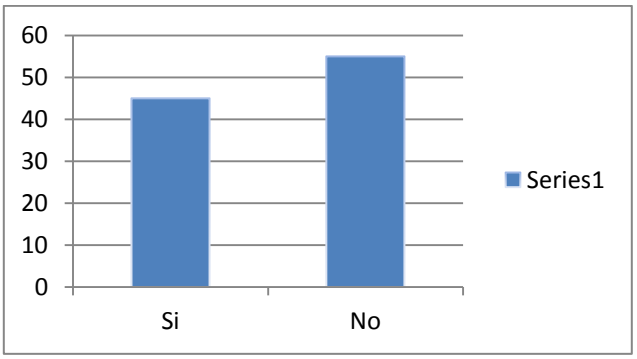


Figura 3. 7. Conocimiento de la informática forense por profesionales del área de derecho

Fuente: Propia

La figura 3.7. se puede observar que el 70% de los profesionales del área de derecho desconocen la ciencia de la informática forense, y un 30% tiene conocimiento de esta. Lo que hace ver que en nuestro medio aún no se tiene suficiente conocimiento de la nueva ciencia forense.

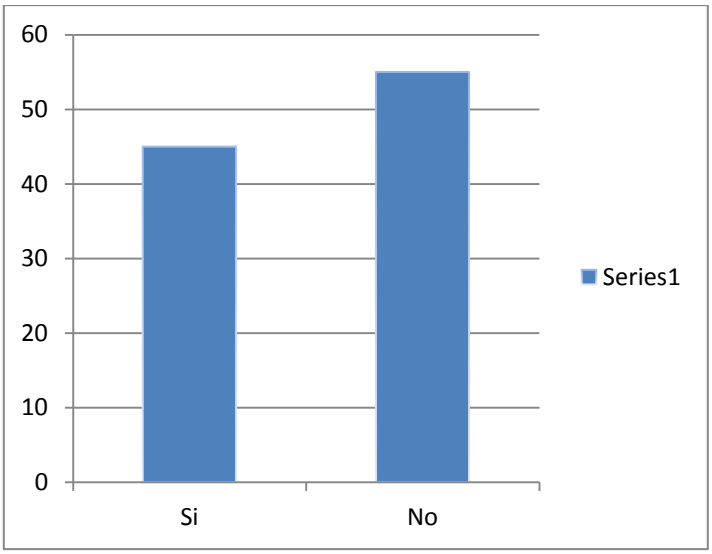


Figura 3. 8.Aplicación de Técnicas Forenses

Fuente: Propia

De acuerdo a la figura 3.8. se puede observar que solo el 15% de profesionales de área de derecho a utilizado en su vida profesional alguna técnica forense durante el proceso de investigación de casos ilícitos en los que se vio involucrada la tecnología. Y el 85% no atendió casos referidos a lo tecnológico por lo cual desconocen la aplicación de estas técnicas.

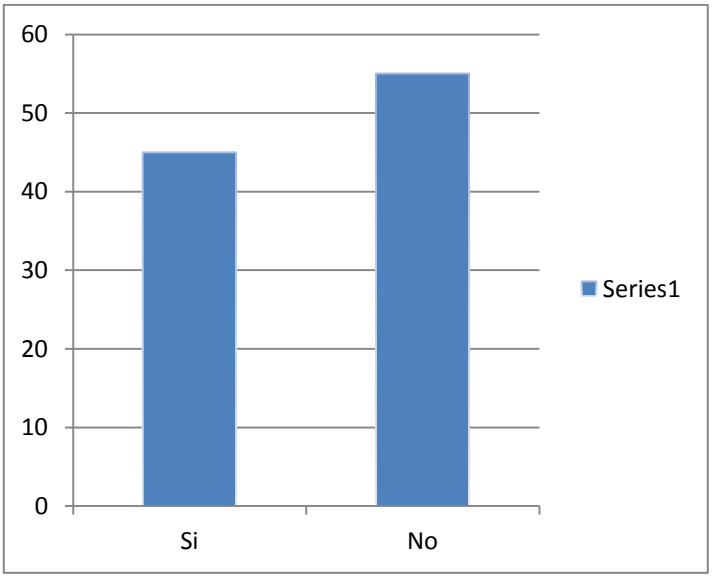


Figura 3. 9.Conocimiento de casos ilícitos en los que ha estado involucrado un dispositivo móvil

Fuente: Propia

Como se puede percibir en la figura 3.9. solo el 10% de los profesionales encuestado conocen casos ilícitos en los que se vio involucrado un dispositivo móvil.

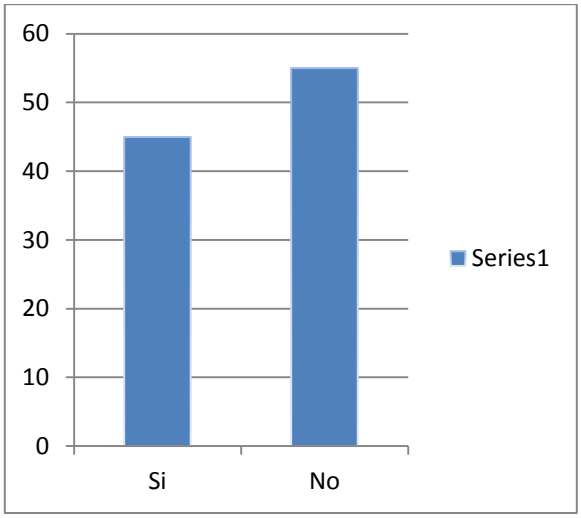


Figura 3. 10.Conocimiento de Evidencia Digital

Fuente: Propia

Observando los resultados de la figura anterior se puede percibir que el 95% de los encuestados desconocen lo que es la evidencia digital.

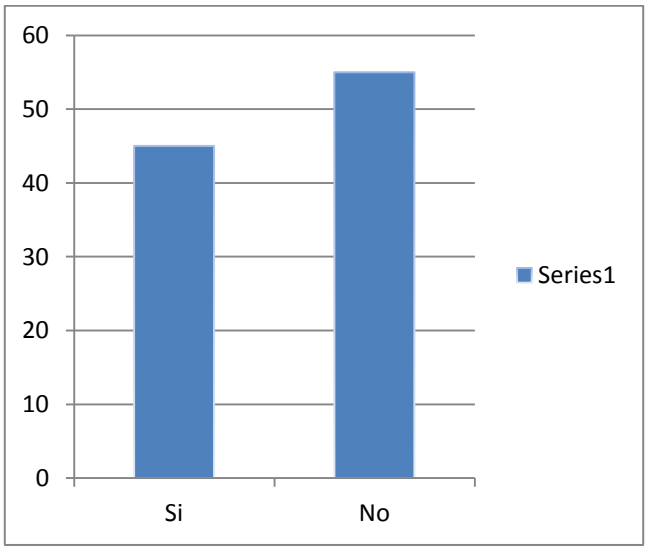


Figura 3. 11.Importancia del conocimiento de herramientas para la recolección de evidencia digital en dispositivos móviles

Fuente: Propia

La figura 3.11. muestra que el 75% de los encuestados consideran que es suma importancia contar con herramientas (metodologías) que ayuden al esclarecimiento de delitos informáticos en los que se ve involucrado un dispositivo móvil. Y un 25% considera que no es tan relevante este tipo de herramientas.

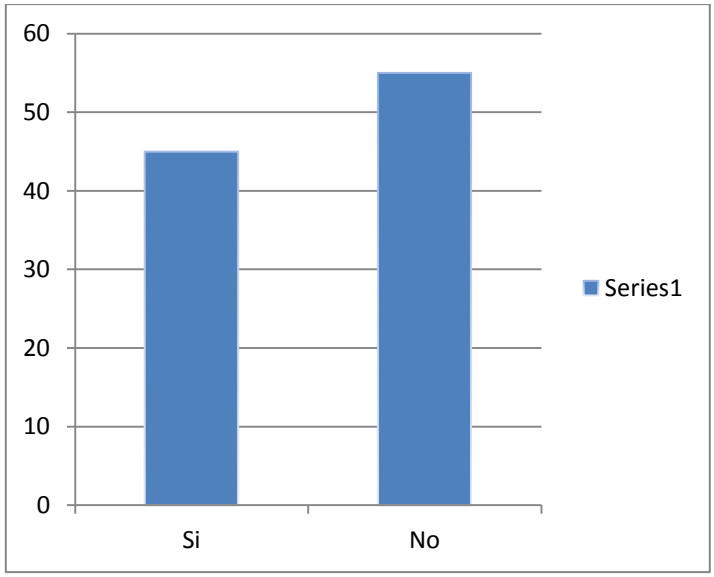


Figura 3. 12.Conocimiento de normas que penalizan los delitos informáticos en Bolivia

Fuente: Propia

La figura 3.12. se puede aseverar que el 45% de los encuestados afirman que conocen de las normas bolivianas en las que se regula el delito informático; sin embargo el 55% desconoce la actual Ley 164 en la que se establece algunos parámetros para el tratamiento de este tipo de casos ilícitos.

De los gráficos anteriores se puede concluir que en nuestro medio aun se desconoce la ciencia de la informática forense y la aplicación de sus técnicas.

Esto hace ver que es necesario socializar más los delitos informáticos ocurridos en nuestro país, además de hacer conocer a la población el impacto que tienen este tipo de casos ilícitos. El uso de internet y telefonía móvil han incrementando de forma vertiginosa lo cual hace pensar que así como estos pueden brindar muchas bondades

también pueden ser utilizados por personas mal intencionadas. Por lo mencionado se ve la necesidad de contar con herramientas (metodologías) que ayuden el proceso de investigación de este tipo de casos. Los resultados anteriormente especificados se los obtuvo de acuerdo a la entrevista realizada a diferentes profesionales del área de derecho (ANEXO N °1)

3.2. Metodología de recolección de evidencia digital en dispositivos móviles (celulares GSM)

En esta sección del documento se presenta la propuesta de la metodología de recolección de evidencia digital en dispositivos móviles (celulares GSM) la cual es el resultado de la revisión y entendimiento de los conceptos expuestos anteriormente. De forma resumida la metodología se divide en cuatro fases principales: Preparación, recolección de datos, análisis de datos y reporte.

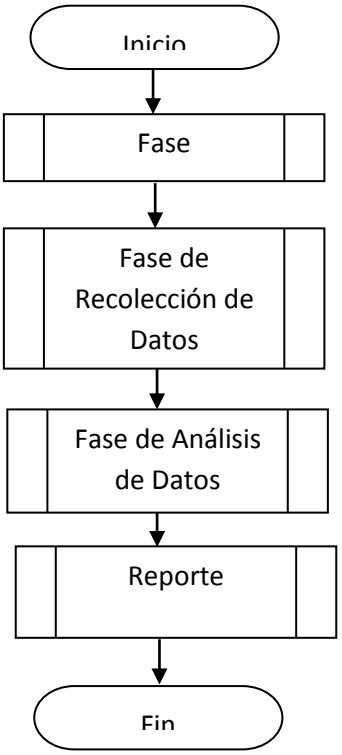


Figura 3. 13. Las cuatro fases de la metodología de recolección de evidencia digital en dispositivos móviles (celulares GSM)

Fuente: Propia

3.2.1. Fase Preparatoria

La fase de preparación es necesariamente la primera que se debe efectuar al realizar un análisis forense orientado a la recolección de evidencia digital en dispositivos móviles (celulares GSM).

Principalmente trata de la preparación de todos los elementos necesarios para efectuar con éxito el proceso, entre los que se encuentra preparar la escena (identificación), el dispositivo (incautación y preservación de evidencia), las herramientas forenses y el personal.

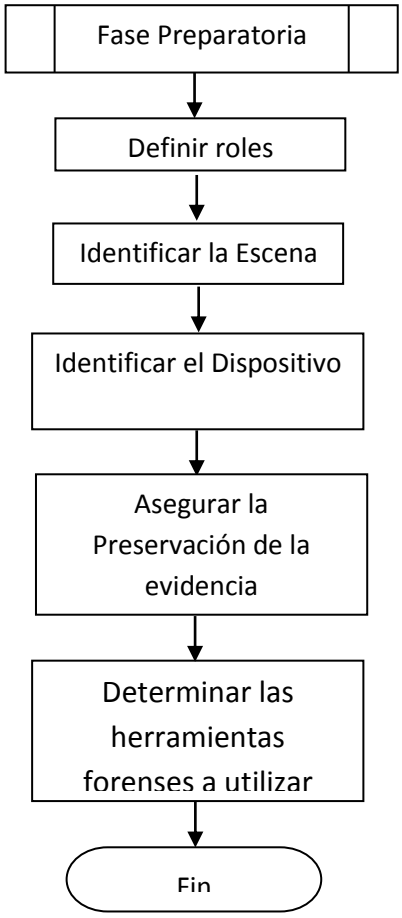


Figura 3. 14.Secuencia de pasos de la Fase Preparatoria

Fuente: Propia

3.2.1.1. Definir roles: Sin importar el tipo del incidente, la variedad de roles involucrados son similares. Antes de comenzar un proceso investigativo de tipo forense, es importante definir una serie de roles entre el personal involucrado con el objetivo de definir responsabilidades y generar un orden en todo el proceso. Además de esto, es importante para generar la cadena de custodia de la evidencia, debido a que dependiendo del rol, la persona puede o no tener acceso a la evidencia asegurando en cierta forma la admisibilidad de la evidencia y su preservación.

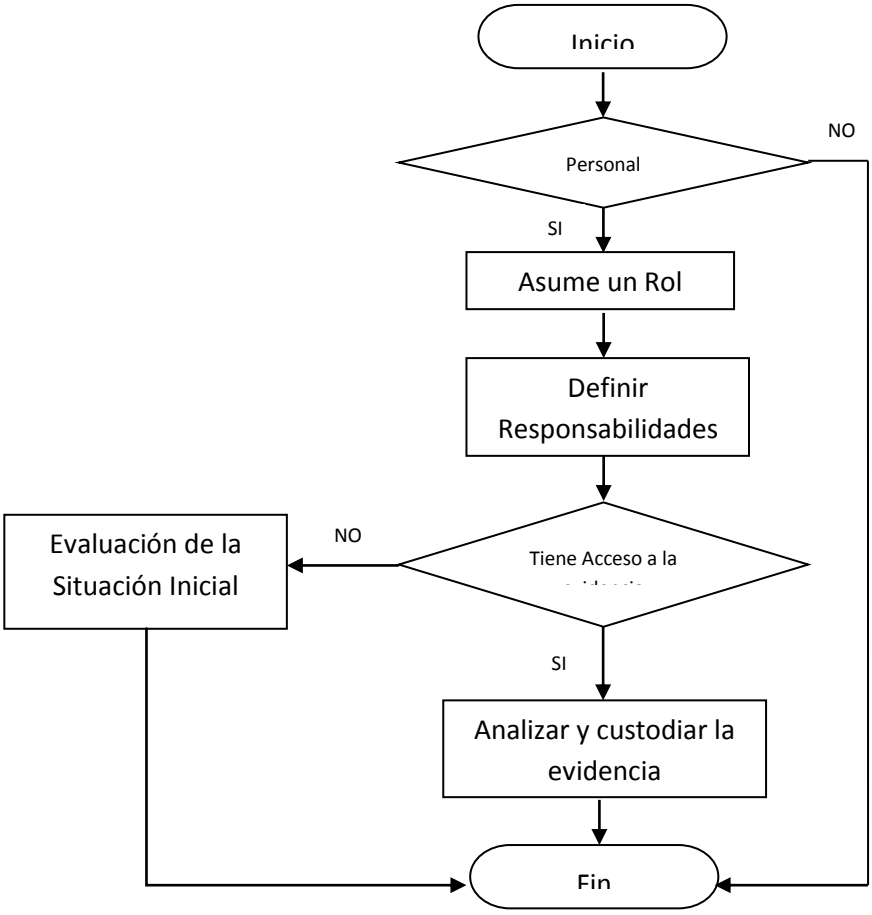


Figura 3. 15.Secuencia de pasos para establecer los roles

Fuente: Propia

3.2.1.1.1. Personal de emergencia

Es personal entrenado, el cual llega primero a la escena del incidente, provee una evaluación inicial de la situación y comienza el nivel apropiado de respuesta. Entre sus responsabilidades se encuentran asegurar la escena del incidente, llamar al personal apropiado para el soporte requerido y asistir con la recolección de la evidencia.

3.2.1.1.2. Investigadores

Son los encargados de planear y manejar la preservación, adquisición, examinación, análisis y reporte de la evidencia digital. El investigador líder está a cargo de supervisar que las actividades ejecutadas en la escena del incidente sean realizadas en el orden y momento correcto.

3.2.1.1.3. Técnicos forenses

Son los encargados de llevar a cabo tareas bajo la supervisión del investigador líder. Los técnicos son responsables de identificar y recolectar toda la evidencia digital, además de documentar todas las acciones realizadas. En realidad son personal especialmente entrenado para incautar el dispositivo conservando la integridad de la evidencia, además de adquirir las respectivas imágenes digitales de la memoria de los dispositivos involucrados. Generalmente, es necesario más de un técnico en la investigación debido a que, usualmente, se necesitan diferentes habilidades y conocimientos.

3.2.1.1.4. Custodios de la evidencia

Son los encargados de proteger toda la evidencia recolectada. Ellos reciben la evidencia recolectada por los técnicos, aseguran que se encuentre propiamente identificada y mantienen una estricta cadena de custodia.

3.2.1.1.5. Analistas forenses

Son los encargados de evaluar el producto de los examinadores forenses teniendo en cuenta aspectos como significancia y valor probativo en el caso.

3.2.1.2. Identificar la escena

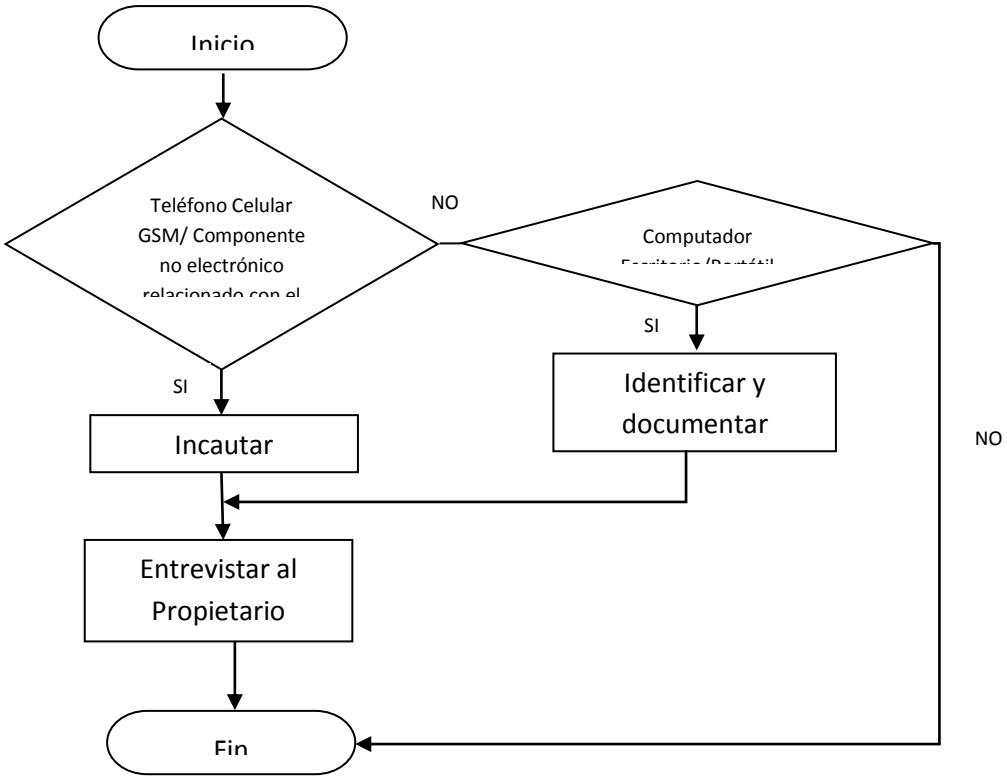


Figura 3. 16.Secuencia de pasos para la identificación de la escena

Fuente: Propia

3.2.1.2.1. Identificar y documentar los componentes electrónicos que no se van a incauta

Los elementos que se deben incautar son, generalmente, teléfonos celulares GSM; sin embargo, es necesario documentar los componentes electrónicos que pueden tener relación con el dispositivo (computadores de escritorio, computadores portátiles, etc..) y que no se van a incautar. La razón de esto es que al buscar los rastros del incidente

es posible que se encuentren datos de conexión o de acceso de éstos dispositivos lo cual, si no existe el registro mencionado anteriormente, puede conllevar a resultados erróneos.

3.2.1.2.2. Recolectar y documentar todos los elementos no electrónicos relacionados con el dispositivo

Ejemplos de estos elementos son manuales del dispositivo (teléfono celular GSM), cargadores, memorias extraíbles, códigos de acceso PIN y PUK entre otros. Dichos elementos son importantes para facilitar el acceso al dispositivo, su utilización y pueden posiblemente facilitar las actividades de la investigación.

3.2.1.2.3. Realizar una entrevista al propietario del dispositivo

Consiste en obtener la mayor cantidad posible de información sobre el incidente, además de datos de acceso y utilización del dispositivo. La información proporcionada por el propietario otorgará las pistas iniciales que permitirán comenzar con el posterior proceso de análisis de la información. Es importante resaltar en detalles como sucesos extraños en el dispositivo, ausencia de información, conexiones Bluetooth establecidas, personas y/o dispositivos con los que se realizó emparejamiento vía Bluetooth, conexiones WAP entre otros.

3.2.1.3. Identificar el dispositivo

a. Documentar el estado del dispositivo

i.Encendido/Apagado

ii. Protegido por PIN?

b. Documentar dispositivo

i.Marca

ii. Modelo

iii.Número de teléfono

iv. Operador

v.Número serial (IMEI)

c. Documentar características del dispositivo (manuales)

3.2.1.4. Asegurar la preservación de la evidencia

a. Asegurar que el personal está capacitado para trabajar con dispositivos móviles.

b. Aislar el dispositivo de la red GSM

c. Crear el registro de la cadena de custodia

d. Documentar toda interacción con el dispositivo

e. Tomar una foto o video que exhiba el estado inicial del dispositivo

3.2.1.5. Determinar las herramientas forenses a utilizar

a. Seleccionar las herramientas que soporten el fabricante.

Algunas de las herramientas forenses existentes actualmente para dispositivos GSM.

- ✓ Device Seizure es la única herramienta que permite adquisición física del dispositivo, lo cual es una gran ventaja debido a que permite obtener una mayor cantidad de información lo cual aumenta en gran medida las posibilidades de encontrar evidencia digital relacionada con el incidente ocurrido.
- ✓ Solamente PhoneBase 2 no soporta la adquisición de datos a través de Bluetooth, sin embargo, esto no es tan grave debido a que en este tipo de conexiones los datos se pueden perder en medio de la transmisión.
- ✓ Device Seizure y MOBILedit! son las únicas herramientas que tienen la funcionalidad de visor hexadecimal. Esta característica es importante en el

análisis de incidentes debido a que permite hacer ingeniería reversa y obtener detalles de las posibles aplicaciones maliciosas instaladas.

- ✓ Device Seizure es la herramienta que más modelos de dispositivos soporta, además es la que ofrece la mayor cantidad de accesorios de conexión tales como cables.
- ✓ Device Seixure y Oxygen Forensic Suite son las herramientas que permiten realizar búsquedas de palabras clave. Esto es muy útil al realizar búsqueda sobre volcados de memoria, que es en donde se encuentra toda la información del dispositivo.
- ✓ MOBILedit! Forensics es la única herramienta que no es de sólo lectura, a pesar de que fue diseñada específicamente para realizar análisis forenses.

Es por esto que no se recomienda la utilización de esta herramienta debido a que puede alterar la integridad de los datos y la evidencia digital podría perder admisibilidad.

Teniendo en cuenta lo anterior, Device Seizure es la herramienta que se recomienda para realizar análisis forenses orientados a incidentes en teléfonos celulares GSM.

b. Definir los criterios de selección: Antes de realizar la selección de la herramienta, es necesario definir, por orden de importancia, los criterios a tener en cuenta con el fin de estar de acuerdo con la política de negocio de la empresa. A continuación se nombran algunos de los más comunes:

Usabilidad: La habilidad de presentar datos de forma útil para el investigador.

Completitud: La habilidad de presentar todos los datos al investigador, incluyendo evidencia culpatoria como exculpatoria.

Precisión: Se refiere a la calidad de los resultados que arroja la herramienta y al margen de errores obtenidos.

Determinismo: La habilidad de la herramienta de producir el mismo resultado cuando se proporcionan el mismo conjunto de instrucciones y los mismos datos de entrada.

Verificable: La habilidad de asegurar la precisión del resultado arrojado por la herramienta teniendo acceso a inmediato a la presentación y traducción de resultados.

Criterios definidos por Daubert:

Prueba: ¿La herramienta ha sido probada empíricamente?

Aceptación: ¿La herramienta ha sido sujeta a revisión antes de ser publicada?

Tasa de error: ¿Cuál es la potencial tasa de errores?

Credibilidad: ¿Cuál es la calificación y estatus de la que tiene la comunidad científica sobre la herramienta?

Claridad: ¿Los resultados proporcionados por la herramienta son fáciles de entender?

Otros criterios:

Calidad: Soporte técnico, fiabilidad y actualizaciones periódicas frecuentes.

Capacidad: Características que soporta, numero de modelos de dispositivos, flexibilidad y personalización.

Asequibilidad: Costo versus beneficios en productividad.

c. Diligenciar lista de chequeo de funcionalidades: Los ítems de la primera lista de chequeo son obligatorios para lograr tener acceso a la herramienta. Si alguno de estos no cumple, no es posible emplear el kit de herramientas en el análisis del dispositivo. El primer ítem es el de mayor importancia debido a que la más importante característica de una herramienta forense es que proteja la integridad de la información accedida. El segundo ítem en importancia es el soporte del dispositivo debido a que si no lo soporta, la herramienta no sirve para realizar el análisis. El tercer ítem está relacionado con la adquisición física de datos. Este ítem es deseable debido a que es importante recolectar la mayor cantidad de información disponible, incluido un volcado de la memoria volátil, para lograr obtener detalles del incidente ocurrido. Finalmente se encuentra el ítem del presupuesto el cual se encuentra de último debido

a que se puede obtener financiación o buscar otras soluciones para adquirir el kit de herramientas.

Los ítems de la segunda lista de chequeo pueden ser opcionales; sin embargo, van ordenados de mayor a menor importancia, de arriba hacia abajo. Debido a la cantidad de datos raw para analizar en un incidente con un dispositivo móvil GSM, el ítem más importante es el de búsqueda de palabras claves y bookmark, lo cual facilitaría la labor en seguida se encuentra la verificación de integridad de los archivos, lo cual ayuda a comprobar que los datos obtenidos son idénticos bit a bit.

A continuación se encuentra el servicio de actualización y soporte técnico, el cual es variable en cuanto a la cantidad de tiempo que dura este ítem y, de acuerdo a esto, adquiere más valor en la lista de chequeo.

Los ítems de la tercera lista de chequeo son los más opcionales. En el primer lugar se encuentra la funcionalidad de visor hexadecimal, el cual es útil en caso que la herramienta no soporte la adquisición física. En seguida se encuentra la funcionalidad de realizar data carving lo cual puede revelar rastros de archivos dejados por códigos maliciosos, lo mismo aplica para la recuperación de archivos borrados. Finalmente se encuentra la funcionalidad de generar reportes en formatos estándar que permitan la presentación de la evidencia de una forma personalizada y entendible para que sea admisible en las instancias judiciales respectivas.

d. Aplicar proceso de prueba a las herramientas seleccionadas: La comunidad de las ciencias forenses digitales esta actualmente creciendo y las tasas de errores para las herramientas forenses necesitan ser continuamente revaluadas a medida que la tecnología cambia. Esto es más difícil en el caso de las ciencias forenses aplicadas a dispositivos móviles, debido a que estos tipos de dispositivos son propietarios.

Es por eso que existe un planteamiento que usa bases de datos, el cual puede ser utilizado para almacenar datos sobre la adquisición de evidencia electrónica en teléfonos móviles, enmarcado en un proceso de prueba de herramientas forenses. En algunas ocasiones, es recomendable hacer uso de este modelo para realizar pruebas más exhaustivas de las herramientas ha utilizar.

3.2.2. Fase de Recolección de Información

Consiste en la recolección de la evidencia digital. Esta fase la realizan los técnicos forenses y se debe tener especial cuidado en la preservación de la integridad y, por tanto, admisibilidad de la evidencia digital.

3.2.2.1. Recolección de evidencia

3.2.2.1.1. Obtención de la imagen de datos:

3.2.2.1.1.1. Adquisición física

Obtención del volcado de memoria tanto volátil como no volátil, es decir, copia bit a bit de la memoria del dispositivo. También es recomendable obtener una imagen de la SIM card debido a que es posible que se encuentren rastros del incidente en dicho dispositivo de almacenamiento.

3.2.2.1.2. Adquisición lógica

Consiste en la obtención de información del tipo lista de contactos, historial de mensajes, fotos, videos etc..

a. Verificación de la integridad de la imagen de datos

b. Creación de una copia de la imagen de datos

c. Aseguramiento de la imagen suministrada

3.2.3. Fase de Análisis de Datos

Consiste en el análisis de los datos recolectados por los técnicos forenses. Esta fase es efectuada por los investigadores forenses y, en general, se identifican los datos tanto físicos como lógicos para construir una línea de tiempo en donde se correlacionen todos los hechos y se pueda obtener la mayor cantidad de detalles del incidente ocurrido.

3.2.3.1. Análisis de la evidencia

a. Identificar propiedades generales de la adquisición

b. Estructura de la adquisición

c. Recuperar los datos borrados

d. Recuperar información oculta

e. Análisis de los datos lógicos

i.Identificadores del dispositivo y del proveedor de servicio

ii. Fecha/hora

iii. Lenguaje

iv. Información de la lista de contactos

v.Información del calendario

vi. Mensajes de texto

vii. Registro de llamadas (recibidas, perdidas, marcadas)

viii. Correo electrónico

ix. Fotos /Videos / Audio

x.Mensajes multimedia

xi. Mensajería instantánea y navegación web

xii. Documentos electrónicos

xiii. Identificación procesos en ejecución

xiv. Revisar los logs del sistema

xv. Identificar rastros de conexiones (Bluetooth, irda, cable)

f. Análisis de los archivos obtenidos (correlación de eventos)

g. Construcción de la línea de tiempo definitiva

3.2.4. Reporte

Consiste en documentar todas las acciones, eventos y hallazgos obtenidos durante el proceso. Todo el personal está involucrado en ésta fase y es vital para asegurar la cadena de custodia de la evidencia. Los reportes generalmente son generados por la herramienta que se utiliza en el análisis.

CAPITULO IV

RESULTADOS

4.1. Realización de los escenarios de Ataque

Este escenario consiste en el envío de un archivo malicioso sin la autorización de la víctima. El virus es relativamente nuevo, es llamado comúnmente “isexplayer” y es considerado el primer malware para Symbian S60 tercera edición. La aplicación actúa como un portal pornográfico el cual ofrece diferentes servicios. Una vez el .jar es instalado, el software automáticamente realiza una llamada premium internacional sin la autorización del propietario.

Normalmente la aplicación es descargada de internet a través del protocolo WAP mostrando el siguiente mensaje:

"Free access to: - 500 Hardcore scenes - 100 Full lenght movies - Picture galleries Important! To install iSexplayer you must be at least 18 years old. You must install and run iSexplayer access module to watch the videos on Nintendo DS, You must install and run iSexplayer access module to watch the videos on Apple iPhone, Install iSexplayer"

Sin embargo, para este caso se descargó el archivo de Internet de la siguiente dirección: http://3g6.se/iSexPlayer.jar. Por otro lado, para realizar el envío de archivos se utilizará la herramienta BlueZSpammer el cual utiliza un filtro de direcciones MAC para enviar el archivo a múltiples dispositivos pensando que posiblemente estén emparejados al dispositivo suplantado.

Teniendo en cuenta la información anterior, se procede a realizar el ataque:

1. Descargar el archivo iSexPlayer.jar de la dirección web especificada.

2. Realizar el procedimiento Blue Mac Spoofing

3. Descargar la herramienta BlueZSpammer v2 de la siguiente dirección web http://gospel.endorasoft.es/bluetooth/especificacion-bluetooth/bluez/Files/BlueZSpammer.v2_ src.zip

4. Modificar el filtro MAC de la herramienta para incluir los dispositivos a los cuales se les desea enviar el virus.

4.2. Seguimiento de la Metodología Propuesta

Los resultados son presentados a continuación mediante tablas. Cada tabla muestra los productos obtenidos al ejecutar las Fases de la Metodología.

La tabla siguiente contiene los pasos relacionados con la primera fase de la metodología. Un aspecto importante es que se cuenta con el personal y equipo para llevar a cabo la aplicación de la metodología.

FASE PREPARATORIA
1. Definir Roles Para la presente investigación forense, se llevara a cabo una distribución de roles acorde con el modelo propuesto por esta metodología. Teniendo en cuenta que el grupo de análisis cuenta con recursos limitados tanto de personal como económicos, se tendrán en cuenta solamente 4 de los 6 roles propuestos inicialmente. Estos roles serán asumidos por la autora de la investigación en curso, y serán los siguientes: a. Investigador b. Custodio de la evidencia c. Examinador forense d. Analista forense

FASE PREPARATORIA

2. Identificación de la escena

2.1. Identificar y documentar los componentes electrónicos que se van a incautar:

Sólo se encontró un dispositivo móvil (teléfono celular GSM)

Tipo	***Marca***	***Modelo***	***Tipo***	***Número de Serie***	***Dirección del Bluetooth***
Teléfono Celular	Nokia	N73-5	RM-132	0543741F01482	00:1A:DC:10:51:E3
Bluetooth Dongle	Encore	USB Dongle	EDR 2.0	50126120000047	00:18:0F:16:2F:70

Tabla N° 1: Características del dispositivo móvil

Fuente: Propia

2.2. Identificar y documentar los componentes electrónicos que no se van a incautar:

No aplica.

2.3. Recolectar todos los elementos no electrónicos relacionados con el dispositivo

Tipo	***Marca***	***Referencia***	***Número de Serie***	***Razón de la Incautación***
Cargador	Nokia	AC-3U	N/A	Facilita la alimentación de energía del dispositivo.
Cable USB	Nokia	CA-53	108882732450	Cable utilizado por el propietario para sincronizar datos.

Tabla N° 2: Características de Dispositivos no Elextrónicos

Fuente: Propia

- ✓ No se encontraron manuales en la escena por lo que se recurrirá a los que se encuentran disponibles en internet. Tampoco se encontraron los códigos PIN y PUK; sin embargo, no son necesarios debido a que el dispositivo se encontraba encendido y además se encontró el cargador que permite proporcionarle energía al dispositivo previniendo que se apague y se pierda la posible evidencia digital residente en la memoria volátil.

2.4. Realizar una entrevista al propietario del dispositivo:

1. Desde cuando es propietario del dispositivo?

R.- Desde aproximadamente un año.

2. Lo compro nuevo o usado?

R.- Lo compre nuevo sellado en caja. Luego abrí las bandas para poder utilizarlo con Tigo debido a que tenía esta línea desde antes.

3. Usualmente que uso le da a su teléfono celular?

R.- Básicamente lo utilizo para comunicarme. Debido a que mi trabajo requiere de movilidad, guardo información importante en él como son documentos PDF. Además de esto, tengo números de celular muy influyentes, por lo que dicha información puede considerarse muy sensible.

4. Utiliza frecuentemente la tecnología Bluetooth?

R.- Muy frecuentemente. Utilizo la gran mayoría del tiempo manos libres Bluetooth, incluso escucho música con el.

5. Sincroniza el contenido de su teléfono con algún computador en especial. Cómo realiza este procedimiento?

R.- Si, utilizo mi computador personal para sincronizar mi agenda y tener una copia de seguridad de mis datos. Para esto utilizo el cable que venía en el teléfono.

6. Además de las conexiones con el manos libres, ¿Ha utilizado últimamente Bluetooth con algún otro dispositivo?

R.-Si, usualmente trasfiero archivos entre mi celular y el de un compañero de trabajo que busca en internet videos o fotos graciosas y me las manda.

7. ¿Dentro de los últimos días alguien mas ha tenido acceso a su manos libres?

R.-Si, usualmente algunos compañeros me lo piden prestado en horas de trabajo para escuchar música, o incluso algunos me lo piden para salir momentáneamente de la oficina en sus automóviles.

FASE PREPARATORIA

8. ¿Ha notado la ausencia de algún tipo de información (fotos, videos, mensajes, contactos, documentos) que se encontraba almacenada en su teléfono celular?

R.- No

9. ¿Realiza alguna otra conexión con su teléfono celular distinta a las ya mencionadas?

R.- No

(**ANEXO N° 2**)

3. Identificación del dispositivo:

3.1. Documentar el estado del dispositivo

a. Prendido/Apagado: El dispositivo se encontraba prendido.

b. Protegido por PIN: El dispositivo se encuentra protegido por PIN.

3.2.Documentar dispositivo

a. Marca: Nokia

b. Modelo: N73

c. Número de teléfono: 3003606608

d. Operador: Tigo

e. Número serial (ESN): 0543741F01482

3.3. Documentar características del dispositivo:

Cobertura

- Modo dual WCDMA/GSM y cobertura GSM de cuádruple banda en los cinco continentes (redes WCDMA2100/EGSM850/900/1800/1900)
- Cambio automático de una banda a otra y de un modo a otro

Dimensiones

- Peso: 116 g
- Altura: 110 mm
- Anchura: 49 mm
- Grosor(max): 19 mm

Funciones de memoria

- Memoria dinámica interna de 42 MB para contactos, mensajes de texto,

mensajes multimedia, tonos de llamada, imágenes, secuencias de vídeo, notas de la agenda, lista de tareas pendientes y aplicaciones

- Admite una tarjeta de memoria miniSD (con función hot swap)
- Ejemplo de capacidad de memoria con tarjeta de memoria miniSD de 1 GB
- Vídeo (MPEG4 CIF a 15fps audio AAC) hasta 175 min.
- Fotos (3,2 megapíxeles) hasta 1.000 fotos
- Música (eAAC+) hasta 1.000 canciones

La oferta de aplicaciones puede variar. Memoria dinámica significa que la memoria disponible es compartida entre las funciones de la memoria dinámica. Cuando se utiliza cualquiera de esas funciones, queda menos memoria disponible para otras funciones también dependientes de la memoria dinámica.

Pantalla e interfaz de usuario

- Espera activa: los principales servicios siempre a mano
- Interfaz de barra de herramientas activa en cámara y galería
- Editor de imágenes y editor de vídeo (manual y automático) en el dispositivo)
- Gran pantalla TFT brillante en color de 2,4 pulgadas QVGA (240 x 320 píxeles) con hasta 262.144 colores
- Detector de luz ambiental: utilizado para optimizar el consumo de energía y el brillo de la pantalla
- Tecla de visualización para el acceso directo a los vídeos e imágenes
- Tecla multimedia para el acceso directo a aplicaciones predefinidas
- Secuencia de imágenes desde la galería con efecto Ken Burns (arrastre y zoom automático) y altavoces estéreo con efecto 3D
- Software Serie 60

Administración de llamadas

- Marcación rápida
- Marcación por voz y comandos de voz
- Nokia Función “Pulsa y habla” (PoC) (Consultar la disponibilidad del servicio con el operador).

- Contactos: base de datos de contactos avanzada que admite múltiples datos de dispositivo y correo electrónico por registro, también imágenes en miniatura y grupos.
- Registros de llamadas: guarda la lista de tus llamadas enviadas, recibidas y perdidas
- Rellamada automática
- Respuesta automática (funciona sólo con kit manos libres portátil o kit de coche compatible)
- Admite número fijo de marcación, que sólo permite las llamadas a los números predefinidos
- Llamada multiconferencia

Tiempos de funcionamiento

- Tiempo en conversación (ECTEL): hasta 226 min. (WCDMA) / 246 min. (GSM)
- Tiempo en espera (ECTEL): hasta 370 horas (WCDMA) / 350 horas (GSM)
- Imágenes estáticas: hasta 800 imágenes (3,2 megapíxeles)
- Captura de vídeo hasta 186 min. (CIF, 15fps)
- Videollamadas hasta 150 min.
- Reproducción de vídeo hasta 366 min. (CIF, 15fps)
- Reproducción de música hasta 12,6 horas (modo offline)
- La autonomía de las baterías puede variar en función de la tecnología de acceso de radio, la configuración de la red del operador y el uso.

Productividad

- Visualizadores de documentos Quickoffice.
- Adobe PDF Reader
- Administración de la información personal: Contactos, Agenda, Tareas Pendientes, Notas, Grabadora, Calculadora, Reloj, Convertidor, Impresión
- Sincronización con PC mediante Nokia PC Suite: Local/Remota (Windows 2000, XP).

- Datos: Agenda, Contactos, Tareas Pendientes, Notas
- Aplicaciones para PC: Microsoft Outlook (2000, 2002, 2003), Outlook Express, Lotus Organizer (5.0, 6.0), Lotus Notes (5.0, 6.0)
- Cliente de correo electrónico con datos adjuntos
- Asistente de Configuración/Configurador de Puntos de Acceso

Navegación y Mensajería

- Navegador de Internet: XHTML, HTML
- Correo electrónico (SMTP, IMAP4, POP3), MMS, SMS

Conexiones

- Pop-PortTMcon conexión USB 2.0 de alta velocidad
- Tecnología Bluetooth 2.0
- Infrarrojos

Transmisión de datos

- WCDMA 2100 con voz y paquetes de datos simultáneos (PS velocidad máxima UL/DL= 128/384 kbps, CS velocidad máxima 64 kpbs)
- Modo de Transmisión Dual (DTM) que admite conexiones de voz y paquetes de datos simultáneas en redes GSM/EDGE
- Velocidades de transmisión de paquetes de datos WCDMA: UL (ascendente) 384kbps, DL (descendente) 384kbps
- Datos de circuito hasta 64kbits/s para videollamadas
- EGPR clase B, intervalos múltiples clase 11 (ascendente 118,4 kbps, descendente 236,8 kbps)
- Códecs de voz admitidos: FR, EFR, WCDMA y GSM AMR
- Aplicación de transmisión de datos para mover datos desde un antiguo dispositivo Nokia S60 compatible mediante una conexión Bluetooth

Las velocidades alcanzadas realmente pueden variar en función del soporte de la red.

Software Adicional

- Java: MIDP2.0, CLDC 1.1, 3D API, PIM API, acceso a archivos API
- Kits de creación de software C++ y Java

FASE PREPARATORIA

4. Asegurar la preservación de la evidencia:

4.1. Asegurar que el personal está capacitado para trabajar con dispositivos móviles:

El proceso será realizado por la autora de la investigación.

4.2. Aislar el dispositivo de la red GSM: Este procedimiento se realizó utilizando una bolsa anti estática con lo cual se logró aislar el celular de la red GSM, previniendo la entrada de llamadas, así como el intercambio de datos con el proveedor de servicio durante el examen forense. Se utilizo la bolsa anti estática debido a que ésta cumple con las necesidades de aislamiento necesarias a un costo económico.

5. Determinar las herramientas forenses a utilizar:

5.1. Seleccionar las herramientas que soporten el fabricante:

Para el dispositivo que será analizado a través de la metodología de recolección de evidencia digital en dispositivos móviles (teléfonos celulares GSM), el cual es un Nokia N73, se obtuvo la siguiente lista de herramientas que lo soportan y han sido seleccionadas preliminarmente:

- Device Seizure
- MOBILedit! Forensics
- Oxygen Forensic Suite

5.2.Definir los criterios de selección:

Entre los criterios de selección de la herramienta que se tendrán en cuenta son los siguientes:

- Usabilidad
- Completitud
- Precisión
- Credibilidad
- Calidad
- Capacidad
- Asequibilidad

FASE PREPARATORIA

6.3. Diligenciar lista de chequeo de funcionalidades

Nombre de la herramienta: Device Seizure

Compañía desarrolladora: Paraben Corporation

ITEMS OBLIGATORIOS	***CUMPLE***	***NO CUMPLE***
Es una herramienta de solo lectura?	X	
Soporta el dispositivo?	X	
Realiza adquisición física?	X	

ITEMS PRIMER GRADO	***CUMPLE***	***NO CUMPLE***
Permite búsqueda de palabras claves?	X	
Realiza verificación de integridad de archivos?	X	
Proporciona frecuentemente actualizaciones y soporte técnico?	X	

ITEMS SEGUNDO GRADO	***CUMPLE***	***NO CUMPLE***
Soporta visor hexadecimal?	X	
Realiza DataCarving?	X	
Recupera Información Borrada?	X	
Permite generar reportes en formato estándar? XML, DOC,PDF.	X	

FASE PREPARATORIA

Nombre de la herramienta: MOBILedit! Forensics

Compañía desarrolladora: COMPELSON Laboratories

ITEMS OBLIGATORIOS	***CUMPLE***	***NO CUMPLE***
Es una herramienta de solo lectura?		X
Soporta el dispositivo?	X	
Realiza adquisición física?		X

ITEMS PRIMER GRADO	***CUMPLE***	***NO CUMPLE***
Permite búsqueda de palabras claves?		X
Realiza verificación de integridad de archivos?	X	
Proporciona frecuentemente actualizaciones y soporte técnico?	X	

ITEMS SEGUNDO GRADO	***CUMPLE***	***NO CUMPLE***
Soporta visor hexadecimal?	X	
Realiza DataCarving?		X
Recupera Información Borrada?	X	
Permite generar reportes en formato estándar? XML, DOC,PDF.	X	

FASE PREPARATORIA

Nombre de la herramienta: Oxygen Forensic Suite

Compañía desarrolladora: Oxygen Software

ITEMS OBLIGATORIOS	***CUMPLE***	***NO CUMPLE***
Es una herramienta de solo lectura?	X	
Soporta el dispositivo?	X	
Realiza adquisición física?		X

ITEMS PRIMER GRADO	***CUMPLE***	***NO CUMPLE***
Permite búsqueda de palabras claves?	X	
Realiza verificación de integridad de archivos?		X
Proporciona frecuentemente actualizaciones y soporte técnico?	X	

ITEMS SEGUNDO GRADO	***CUMPLE***	***NO CUMPLE***
Soporta visor hexadecimal?		X
Realiza DataCarving?		X
Recupera Información Borrada?		X
Permite generar reportes en formato estándar? XML, DOC,PDF.	X	

- ✓ Se tomaron fotografías digitales y video sobre el estado de la escena, además se generó una esquematización sobre el estado de la escena.

(**ANEXO N° 3**)

RESUMEN: Se ha obtenido información del equipo incautado y del propietario del dispositivo móvil.

DOCUMENTOS /ARCHIVOS: Imágenes digitales.

FASE DE RECOLECCIÓN DE LA INFORMACIÓN

Recolección de evidencia

Obtención de la imagen de datos:

1. Adquisición física: Device Seizure es la única herramienta en el mercado que actualmente puede realizar una adquisición física de datos, la cual es mucho más detallada que la lógica debido a que obtiene una copia bit a bit del almacenamiento físico entero, lo cual incrementa las posibilidades de encontrar rastros del ataque. Este procedimiento no fue posible realizarlo debido a que el soporte de Paraben no proporcionó una forma de realizarlo por lo que queda la duda de si realmente la herramienta es capaz de realizar dicho procedimiento, por lo menos con el teléfono celular Nokia N73.

2. Adquisición lógica: El procedimiento de obtención de la imagen fue realizado satisfactoriamente siguiendo los siguientes pasos:

Selección del fabricante: Se seleccionó la opción Nokia Symbian OS 9.x debido a que éste es el sistema operativo del dispositivo que se va a examinar. Existen otras opciones como son Nokia GSM pero no obtienen datos relevantes y son diseñadas más que todo para otros modelos de Nokia.

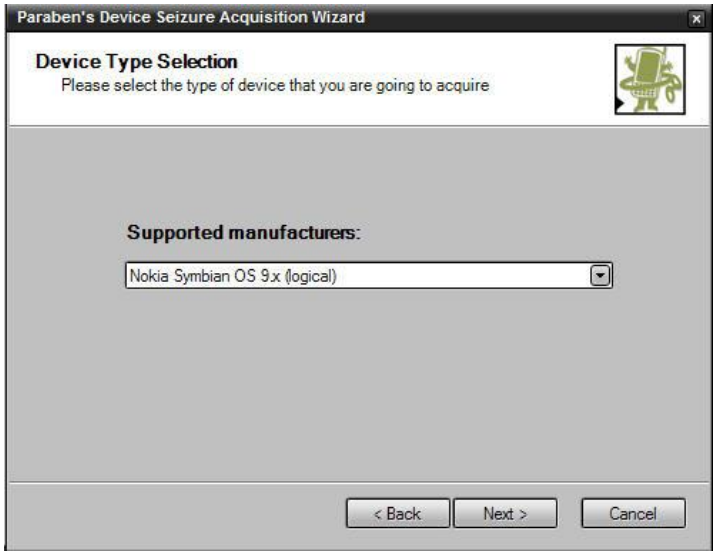


Figura 4. 1.Selección del fabricante en la herramienta Device Seizure
Fuente: Propia

FASE DE RECOLECCIÓN DE LA INFORMACIÓN

Selección del tipo de conexión: Debido a que el dispositivo estaba conectado utilizando el cable USB de referencia CA-53, la única forma de conexión era USB.

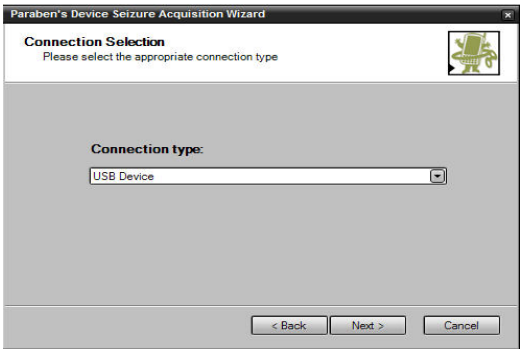


Figura 4. 2.Selección del tipo de conexión en la herramienta Device Seizure
Fuente: Propia

Tipos de datos: Debido a que al seleccionar los dos tipos de datos, la herramienta entraba en conflicto con el sistema operativo y reiniciaba el computador, fue necesario seleccionar uno por uno y tener dos imágenes de datos, una para File System y otra para Backup and Private Data.

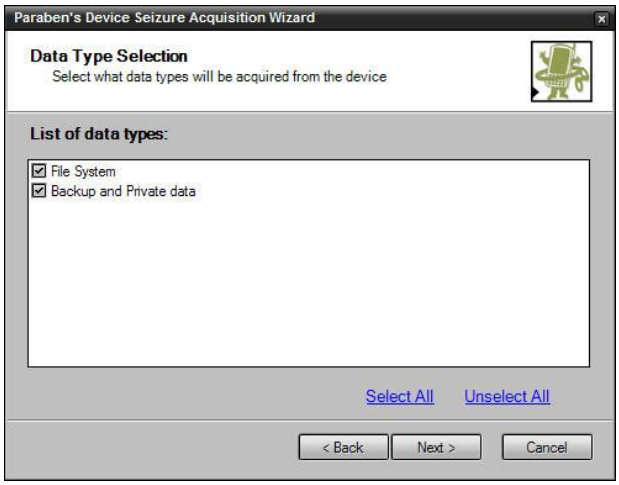


Figura 4. 3. Selección del tipo de datos que se desean obtener en la herramienta Device Seizure
Fuente: Propia

Verificación de la integridad de la imagen de datos: Esta sección no aplica para el presente caso debido a que la imagen se obtiene directamente a través de la herramienta y no es proporcionada por otra entidad externa.

FASE DE RECOLECCIÓN DE LA INFORMACIÓN

Creación de una copia de la imagen de datos: Se realizaron tres copias de las dos imágenes lógicas de datos obtenidas del dispositivo. Cada una de ellas fue almacenada en un computador diferente para evitar la pérdida o modificación de la posible evidencia digital almacenada.

Aseguramiento de la imagen suministrada: La imagen suministrada se encuentra almacenada en un lugar oculto en cada uno de los computadores personales los cuales requieren de una contraseña para acceder.

Datos Recolectados:

Device Seizure:

Directorio. En cuanto a la información sobre el directorio almacenado en el equipo de telefonía celular modelo N73-5. Se tiene el siguiente resumen:

- Presenta 25 contactos almacenados en la memoria interna del equipo.
- Presenta 77 contactos almacenados en la tarjeta SIM.

✓ **Registro de Llamadas.** En cuanto al registro de llamadas el equipo presenta al momento de la extracción de datos poca actividad. El programa solo recuperó un registro correspondiente a las llamadas perdidas.

✓ **Tareas Programadas**. Respecto a tareas programadas el programa no encontró ningún evento programado.

✓ **Historial SMS:** El programa logró extraer datos relacionados con la actividad de mensajes SMS. El historial se compone de 264 mensajes de texto.

✓ **Detalles del equipo del equipo N73-5.** Además de haberse identificado el modelo comercial del equipo, el programa logró identificar diferentes clasificaciones de modelo del equipo asegurado.

MobilEdit:! Forensics

✓ **Directorio**

- Presenta 25 contactos almacenados en la memoria interna del equipo.
- Presenta 78 contactos almacenados en la tarjeta SIM.

FASE DE RECOLECCIÓN DE LA INFORMACIÓN
• Esta herramienta obtuvo un contacto más que Device Seizure. ✓ **Registro de llamadas.** Similar al programa Device Seizure pues solo se pudo extraer información sobre una llamada perdida. ✓ **Tareas Programadas.** No se encontraron datos sobre esta categoría. ✓ **Historial SMS**. MobilEdit! logró extraer información sobre mensajes SMS. Al igual que device Seizure, el historial está compuesto de 264 mensajes de texto. ✓ **Detalles del equipo N73-5**. Mobiledit también logro identificar diferentes clasificaciones de modelo del equipo asegurado. **PC Suite:** Con esta aplicación se accedió a una tarjeta de memoria externa que acompaña al dispositivo. Se obtuvieron los siguientes elementos. ✓ Se obtuvo un albúm de imágenes digitales. El albúm se compone de 54 archivos. ✓ Imágenes adicionales. Una carpeta que contiene 9 imágenes. ✓ Archivos de audio. • Archivos de tipo mp3. Se encontraron, en total 45. • Archivos de tipo (.mid):Se encontró 1 archivo. ✓ Archivo de tipo (thm). Se encontraron 6 archivos. ✓ Archivos de tipo (3gp): Se encontró 1 archivo. Detectar información eliminada u escondida Las herramientas utilizadas para la extracción de datos (Mobiledit y device Seizure) no permitieron realizar recuperación de datos eliminados.
RESUMEN: En esta etapa se han analizado los objetos de interés para identificar los eventos relacionados con el incidente.
DOCUMENTOS/ARCHIVOS DIGITALES: Tipos de archivos txt.

FASE DE ANÁLISIS

Análisis de la adquisición de datos privados y de respaldo

Identificar propiedades generales de la adquisición:

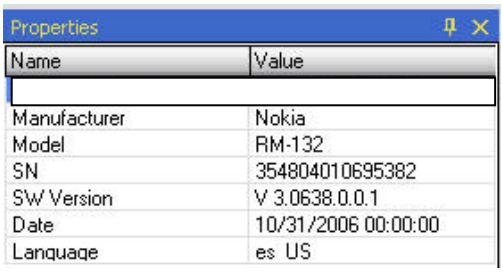


Figura 4. 4.Propiedades generales de la adquisición de datos privados y de respaldo
Fuente: Propia

La imagen muestra los datos principales de la adquisición los cuales son:

- **Marca de tiempo del programa:** Muestra la fecha en que fue realizada la adquisición de datos privados y de respaldo.
- **Fabricante:** Especifica la empresa que fabricó el dispositivo.
- **Modelo:** Expone la referencia del modelo del dispositivo.
- **SN**: Muestra el número de serie del dispositivo que va a ser analizado.
- **SW Versión:** Especifica la versión de software del dispositivo la cual es independiente del modelo y puede ser actualizada mediante el programa de sincronización PC Suite.
- **Date:** Corresponde a la fecha del la versión de software instalada en el dispositivo.
- **Language:** Corresponde a los lenguajes que tiene pre instalados el dispositivo.

Estructura de la adquisición:

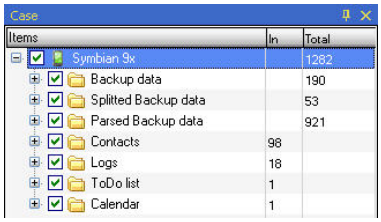


Figura 4. 5. Estructura de la adquisición de datos privados y de respaldo
Fuente: Propia

La imagen anterior muestra la estructura de la adquisición de datos privados y de respaldo en la que se encuentran las siguientes carpetas principales:

- Backup Data: Corresponde a la información de respaldo recolectada del dispositivo examinado.
- Splitted Backup data: Muestra la información obtenida del Backup Data en un formato sin decodificar, es decir, en modo texto plano. Un ejemplo de esto es el siguiente:

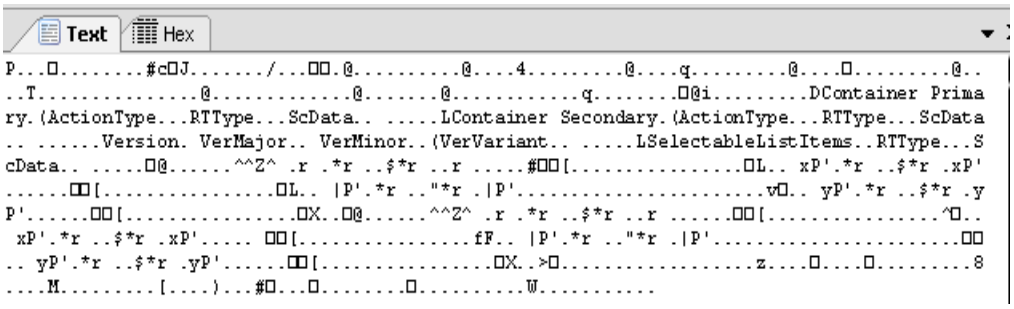


Figura 4. 6. Ejemplo de datos en formato Splitted
Fuente: Propia

Parsed Backup data: Muestra la información decodificada permitiendo que pueda ser leída por personas fácilmente y, así mismo, pueda ser analizada y reportada de una manera más sencilla. Cabe destacar que este proceso es realizado automáticamente para cualquier tipo de datos que lo permitan y que no todos los tipos de datos y no todos los plug-ins pueden ser sometidos a este proceso. Un ejemplo de datos interpretados es:

	CM_Id	CM_Type	CM_PrefTemplateRefId	CM_UIDString
☑	0	268440331	-1	00e0f7c4c2cdaa40
☑	500	268440329	-1	00e131ab29681e69
☑	501	268440329	-1	00e131ab296f4018
☑	502	268440329	-1	00e131ab2973659e
☑	503	268440329	-1	00e131ab2978164d
☑	504	268440329	-1	00e131ab297c14c3
☑	505	268440329	-1	00e131ab2983d717
☑	506	268440329	-1	00e131ab298b2c88
☑	507	268440329	-1	00e131ab298f7b8f
☑	508	268440329	-1	00e131ab29946465
☑	509	268440329	-1	00e131ab29996e6f
☑	510	268440329	-1	00e131ab299e24fa
☑	511	268440329	-1	00e131ab29a2df6d
☑	512	268440329	-1	00e131ab29a896ce
☑	513	268440329	-1	00e131ab29ac9f85
☑	514	268440329	-1	00e131ab29b13bb2
☑	515	268440329	-1	00e131ab29b5392e
☑	516	268440329	-1	00e131ab29ba331b
☑	517	268440329	-1	00e131ab29c018df
☑	518	268440329	-1	00e131ab29c5ad95
☑	519	268440329	-1	00e131ab29ca8ab3

Figura 4. 7. Ejemplo de datos en formato Parsed
Fuente: Propia

- ✓ **Contacts:** Contiene toda la agenda de contactos del dispositivo. Esta se encuentra interpretada y se muestra en forma de tablas de fácil entendimiento y comprensión para su análisis.
- ✓ **Logs:** Contiene la información de los últimos registros de llamadas del dispositivo. Entre ellas se encuentran las llamadas realizadas, perdidas y/o realizadas.
- ✓ **ToDo list:** Contiene la información de la lista de tareas por realizar.
- ✓ **Calendar:** Contiene toda la información del calendario del dispositivo.

Recuperar los datos borrados:

- ✓ Los datos borrados se localizan en las siguientes carpetas:
- ✓ Parsed Backup data: En ella se encuentran los siguientes archivos con filas borradas:

	t		v	x	a	n
☑	0	-09-04 04:23:07	4	2	0	@lang
☑	2	-09-04 04:23:42	0	1	0	xxx

Figura 4. 8. Cambio del lenguaje por defecto de una aplicación
Fuente: Propia

Corresponde al cambio del lenguaje por defecto de la aplicación.

	DType	Flag1	Flag2	Flag3	Flag4	Id	Re	Direction	Duration	St	Sub	Number	Contact	Link	Data
10-21 22:57:31	1	0	0	0	0	2421		0	175	0	0	*300	0	0	Data
10-21 22:50:53	1	0	0	0	0	2420		0	124	0	0	*300	0	0	Data
10-22 21:43:53	1	0	0	0	0	2427		0	6	0	0	*300	0	0	Data
10-21 22:50:26	1	0	0	0	0	2419		0	10	0	0	*300	0	0	Data
10-21 22:45:57	1	0	0	0	0	2418		0	257	0	0	*300	0	0	Data
10-21 22:50:53	1	0	0	0	0	2420		0	124	0	0	*300	0	0	Data
10-22 21:43:53	-1	0	0	0	0	2427		0	0	0	0	*300	0	0	Data
10-21 22:57:31	1	0	0	0	0	2421		0	175	0	0	*300	0	0	Data
10-21 22:50:26	1	0	0	0	0	2419		0	10	0	0	*300	0	0	Data
10-21 22:45:57	1	0	0	0	0	2418		0	257	0	0	*300	0	0	Data
10-21 22:50:53	1	0	0	0	0	2420		0	124	0	0	*300	0	0	Data
10-22 23:20:10	-1	0	0	0	0	2432		0	0	0	0	000000	0	0	Data
10-21 22:57:31	1	0	0	0	0	2421		0	175	0	0	*300	0	0	Data
10-22 22:05:23	-1	0	0	0	0	2431		0	0	0	0	*300	0	0	Data
10-22 21:45:49	-1	0	0	0	0	2428		0	0	0	0	*300	0	0	Data
10-22 21:43:53	1	0	0	0	0	2427		0	6	0	0	*300	0	0	Data
10-22 21:45:49	1	0	0	0	0	2428		0	206	0	0	*300	0	0	Data
10-22 21:58:33	-1	0	0	0	0	2430	Fer	1	0	0	6	3017462314	593	0	Data
10-22 21:58:29	-1	0	0	0	0	2429	Fer	5	0	0	6	3017462314	593	0	Data
10-22 21:43:49	-1	0	0	0	0	2427		0	0	0	0	*300	0	0	Data
10-21 22:45:57	1	0	0	0	0	2418		0	257	0	0	*300	0	0	Data
10-21 22:50:42	-1	0	0	0	0	2420		0	0	0	0	*300	0	0	Data
10-21 22:50:26	1	0	0	0	0	2419		0	10	0	0	*300	0	0	Data

Figura 4. 9. Registro de eventos eliminados del dispositivo
Fuente: Propia

En total son 45 registros los cuales se pueden ver más detalladamente en el reporte generado al final de la presente metodología.

- **Logs:** Contiene el registro de las llamadas realizadas, entrantes y perdidas del dispositivo. A continuación se muestran los registros eliminados:

	Id	Event type	Direction	Contact Id	Number	Remote party	Subject
☑	2430	Voice call	Incoming	593	3017462314	Fer tigo	6
☑	2428	Voice call	Outgoing	0	*300		0
☑	2432	Voice call	Outgoing	0	000000		0
☑	2431	Voice call	Outgoing	0	*300		0
☑	2424	Voice call	Incoming	0	3134968930		0
☑	2422	Voice call	Missed call	0	3134968930		0
☑	2427	Voice call	Outgoing	0	*300		0
☑	2426	Voice call	Incoming	0	3153390295		0

Figura 4. 10. Registro de llamadas del dispositivo
Fuente: Propia

Recuperar información oculta: En esta adquisición, no se encontró ningún rastro de archivos ocultos en el teléfono celular.

FASE DE ANÁLISIS

Análisis de los datos lógicos:

Identificadores del dispositivo y del proveedor de servicio

Identificadores del dispositivo:

- **Fabricante:** Nokia
- **Modelo:** RM-132
- **Serial:** 354804010695382
- **Versión SW:** v3.0638.0.0.1

Proveedor del servicio: No fue posible determinarlo.

• **Fecha/hora:** Según la marca de tiempo de las propiedades de la adquisición, la fecha y hora son: 22/11/2011 07:55:44 PM

• **Lenguaje:** Español – Ingles

• **Información de la lista de contactos:** Se encuentra en la carpeta Contacts. Una muestra de la información obtenida es la siguiente:

	Id	Group	Apellidos	Nombre	Teléfono (casa)	Teléfono (oficina)
☑	563		Marin			
☑	564		Mera			
☑	562		Mama			
☑	560		Malagon			
☑	561		Malagon2			
☑	565		Mera2			
☑	569		Papa			
☑	570		Papa Fer			
☑	568		Oswaldo			
☑	566		Miami			
☑	567		Nena			
☑	559		Luis Niño			
☑	551		James			
☑	552		Jose Luis Gome			
☑	550		Hougton			

Figura 4. 11. Información de la lista de contactos
Fuente: Propia

En total son 77 registros los cuales se pueden ver más detalladamente en el reporte generado al final de la presente metodología.

Información del calendario: La información del calendario se encuentra en la base de datos local C:Calendar. El archivo contiene la información del calendario, sin embargo, no se encuentra interpretado sino que está en formato binario y por lo tanto es complejo de analizar.

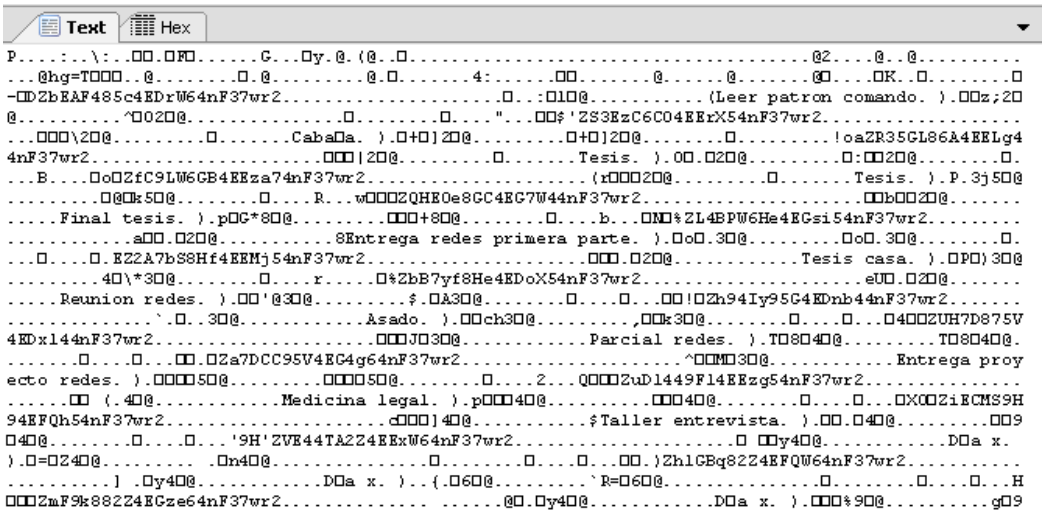


Figura 4. 12. Información del calendario del dispositivo
Fuente: Propia

El archivo completo se puede ver más detalladamente en el reporte generado al final de la presente metodología.

Mensajes de texto: No se encontraron registros de mensajes cortos relevantes.

Registro de llamadas (recibidas, perdidas, marcadas): Se encuentra en la carpeta logs la cual contiene el registro de las llamadas realizadas, entrantes y pérdidas del dispositivo.

	Id	Event type	Direction	Contact Id	Number	Remote party	Subject		Duration
☑	2423	Voice call	Missed call	0	3134968930		0	-10-22 18:24:02	00:00:00
☑	2425	Voice call	Missed call	0	3153390295		0	-10-22 20:51:36	00:00:00
☑	2429	Voice call	Missed call	593	3017462314	Fer tigo	6	-10-22 21:58:29	00:00:00
☑	2421	Voice call	Outgoing	0	*300		0	-10-21 22:57:26	00:00:00
☑	2418	Voice call	Outgoing	0	*300		0	-10-21 22:45:57	00:00:00
☑	2419	Voice call	Outgoing	0	*300		0	-10-21 22:50:22	00:00:00
☑	2420	Voice call	Outgoing	0	*300		0	-10-21 22:50:42	00:00:00

Figura 4. 13. Información del registro de llamadas del dispositivo
Fuente: Propia

Correo electrónico: No se obtuvo información relevante relacionada con correo electrónico en esta adquisición.

Fotos /Videos / Audio: No se obtuvo información relevante relacionada con Fotos, Videos o Audio en esta adquisición.

FASE DE ANÁLISIS

Mensajes multimedia: No se obtuvo información relevante relacionada con mensajes multimedia en esta adquisición.

Mensajería instantánea y navegación web: No se obtuvo información relevante relacionada con mensajería instantánea y navegación web en esta adquisición.

Documentos electrónicos: No se obtuvo información relevante relacionada con documentos electrónicos en esta adquisición.

Identificar procesos en ejecución: No se obtuvo información relevante relacionada con procesos en ejecución en esta adquisición.

Revisar los logs del sistema: A través de la adquisición de los datos privados y de respaldo, se logro obtener una serie de registros de instalación de aplicaciones externas en el sistema. La información se encuentra en el archivo \DBS_10207216_SWInstLog.db.

time	uid	name	vendor	version	action
-664268263 14758502	269963934	xXx: Triple Threat	Sony Pictures	1.01(3)	1
1669034505 14758845	269482456	Blooover2	trifinite.group	1.00(0)	0
-990622638 14758502	269660426	Darts XXX	Future Design Group	1.00(0)	1
-823552513 14758502	269963934	xXx: Triple Threat	Sony Pictures	1.01(3)	0
-1445884519 14759263	269705728	iSexPlayer	Vendor	1.00(0)	0
1040269132 14759508	269681078	MagicBlueHack	Pavel-Avishek	1.00(0)	0
-553622987 14759246	270512361	MMSSync	Nokia	1.00(0)	0
-1776967644 14759263	269710801	iSexPlayer	Vendor	1.00(0)	0
-1113035888 14758502	269660426	Darts XXX	Future Design Group	1.00(0)	0
1431663783 14758502	269691934	Turbo Jet Ski 3D	Gameloft SA -supplied by leo5354-	1.00(1)	0
1832138908 14758502	269946902	Mortal Kombat Mobile 3D By Doru The Shinigami	Games Ltd.	1.01(3)	0
763676633 14758402	-1610612501	black red by alfa	Vendor-EN	1.00(0)	0
985446033 14758502	269760008	Burnout	Electronic Arts/BiNPDA	4.03(37)	0
-1898419513 14758502	536875631	3D miniGolf	3D Arts-EN	1.50(0)	0
-1535007638 14758502	536875631	3D miniGolf	3D Arts-EN	1.50(0)	1
2145299408 14758502	269946902	Mortal Kombat Mobile 3D By Doru The Shinigami	Games Ltd.	1.01(3)	1
-2102084763 14758502	269633437	DTMRD3	Player X	0.04(7)	0

Figura 4. 14. Registro de instalación de aplicaciones en el dispositivo
Fuente: Propia

Identificar rastros de conexiones (Bluetooth, irda, cable): En este paso se realizó la búsqueda de palabras claves específicas del caso en donde se encontraron los siguientes hallazgos relevantes:

- Búsqueda de la palabra log: Se encontró un archivo llamado \DBS_10204058_63ZdrL3JArqmHPrufo8aPFRkDyg- en donde se puede leer un texto sospechoso:

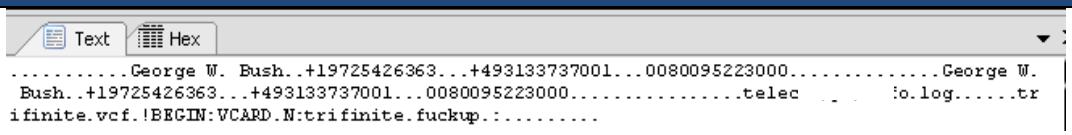


Figura 4. 15. . Texto sospechoso encontrado buscando la palabra "log"
Fuente: Propia

La ruta pb/info.log es propia de un ataque muy conocido realizado a través de Bluetooth llamado Bluesnarfer. Además de esto se observa un nombre y unos números sospechosos, como si se deseara ingresar ese contacto en la lista del dispositivo.

- **Búsqueda de la palabra sync:** Se encontraron varios registros de conexiones realizadas con PC Suite para sincronización de datos. A continuación un ejemplo de datos obtenidos:

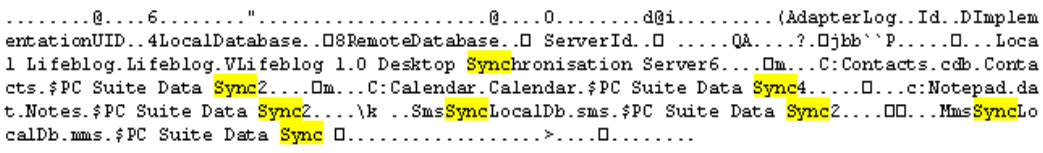


Figura 4. 16. Ejemplo de archivo obtenido buscando la palabra "sync"
Fuente: Propia

En el siguiente archivo, denominado DBS_101F99FB_nsmlagentlog.db se pueden observar más detalles de la conexión y de los tipos de datos sincronizados:

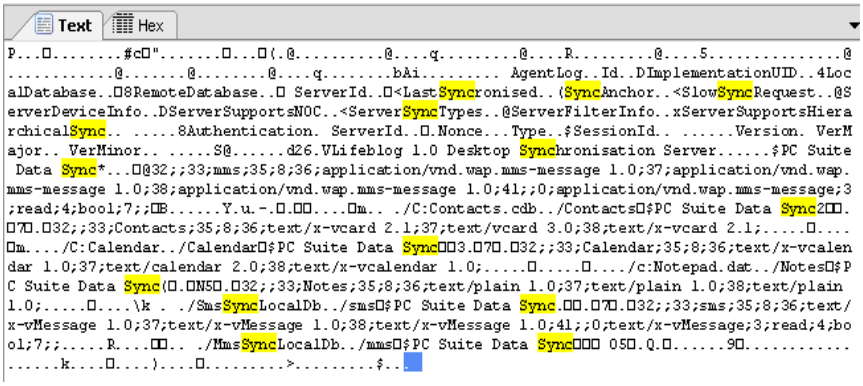


Figura 4. 17. . Detalle del archivo DBS_101F99FB_nsmlagentlog.db en formato splitted
Fuente: Propia

Estos mismos datos se pueden observar interpretados para un mejor entendimiento:

	Id	ImplementationUID	LocalDatabase	RemoteDatabase	ServerId	LastSyncronised	Anchor
☑	4	270560092	./SmsSyncLocalDb	./sms	PC Suite Data Sync		-10-23 00:47:30
☑	5	270512361	./MmsSyncLocalDb	./mms	PC Suite Data Sync		-09-24 03:59:41
☑	3	270501394	./c:Notepad.dat	./Notes	PC Suite Data Sync		-09-24 03:32:42
☑	1	270495197	./C:Contacts.cdb	./Contacts	PC Suite Data Sync		-10-23 00:47:15
☑	2	270495198	./C:Calendar	./Calendar	PC Suite Data Sync		-10-23 00:47:23

Figura 4. 18. Detalle del archivo DBS_101F99FB_nsmlagentlog.db en formato parsed
Fuente: Propia

• Búsqueda de la palabra 00180F: Esta cadena de caracteres corresponde a dirección MAC del otro teléfono celular incautado y a la dirección del adaptador USB (la cual se supone que fue cambiada a la del otro teléfono para realizar una suplantación). El resultado fue el siguiente:

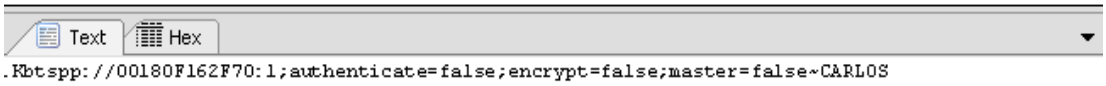


Figura 4. 19. Cadena de texto encontrada buscando la MAC del otro celular incautado
Fuente: Propia

En esta línea se muestra el rastro de una conexión Bluetooth desde esa dirección MAC a través de Bluetooth en donde no se realizó autenticación (debido a que los dispositivos estaban aparentemente autenticados), no se realizó cifrado y el maestro de la conexión no fue el dispositivo analizado sino el que realizó la conexión (esto quiere decir que el archivo fue enviado desde el otro celular). Se realizó la búsqueda de la MAC de manos libres pero no se encontró ningún rastro.

Análisis de la evidencia de la adquisición del sistema de archivos

Identificar propiedades generales de la adquisición:

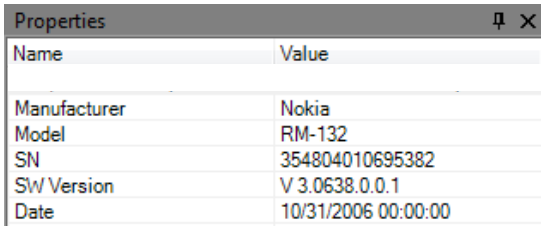


Figura 4. 20. Propiedades generales de la adquisición del sistema de archivos
Fuente: Propia

FASE DE ANÁLISIS

Estructura de la adquisición:

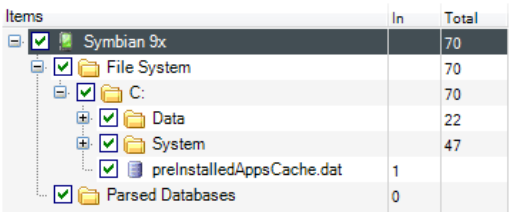


Figura 4. 21.. Estructura de la adquisición del sistema de archivos
Fuente: Propia

La imagen anterior muestra la estructura de la adquisición del sistema de archivos, en la que se encuentran las siguientes carpetas principales:

• **File System:** Carpeta principal del teléfono, sobre la cual se encuentra montado el sistema de archivos del teléfono y sus particiones.

• **C: :** Contiene toda la información de datos de las aplicaciones del teléfono, así como los datos de sistema.

• **Data:** Esta carpeta contiene los datos de las aplicaciones del teléfono, como lo son documentos, juegos, imágenes, instalaciones, sonidos, videos, etc.

• **System:** Esta carpeta contiene datos de sistema, como lo son las bases de datos del sistema, logs, registros, y algunas configuraciones del sistema.

• **Parsed Databases:** Corresponde a archivos binarios interpretados en forma de tablas para permitir un mejor entendimiento e interpretación de la información.

Recuperar los datos borrados: En esta adquisición, no se encontró ningún rastro de archivos borrados en el teléfono celular.

Recuperar información oculta: En esta adquisición, no se encontró ningún rastro de archivos ocultos en el teléfono celular.

Análisis de los datos lógicos :

Identificadores del dispositivo y del proveedor de servicio

Identificadores del dispositivo:

- Fabricante: Nokia
- Modelo: RM-132
- Serial: 354804010695382 • Versión SW v3.0638.0.0.1

FASE DE ANÁLISIS

Proveedor del servicio: No se pudo determinar

- Fecha/hora: Según la marca de tiempo de las propiedades de la adquisición, la fecha y hora son: 22/11/2011 08:51:01 PM
- Lenguaje: Español – Ingles

Información de la lista de contactos: No se obtuvo información relevante relacionada con la lista de contactos en esta adquisición.

Información del calendario: No se obtuvo información relevante relacionada con el calendario en esta adquisición.

Mensajes de texto: No se obtuvo información relevante relacionada con los mensajes de texto en esta adquisición.

Registro de llamadas (recibidas, perdidas, marcadas): No se obtuvo información relevante relacionada con el registro de llamadas en esta adquisición

Correo electrónico: No se obtuvo información relevante relacionada con correo electrónico en esta adquisición

Fotos /Videos / Audio:

Fotos: A través de esta adquisición fue posible recuperar 13 imágenes del teléfono celular vulnerado. Las 13 imágenes fueron halladas en la ruta C:\Data\Images\200809\200809A0\. A través de los nombres de los archivos que contienen el patrón DDMMAAAA###.jpg, es posible determinar que existen imágenes creadas en las siguientes fechas:

- 07/09/2008
- 13/09/2008
- 14/09/2008
- 16/09/2008

Las imágenes encontradas en el teléfono a través de la adquisición son las siguientes**:**

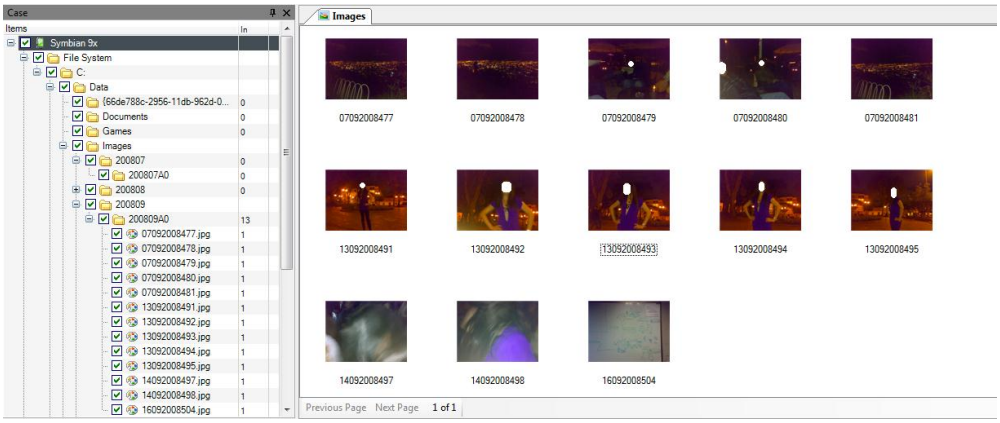


Figura 4. 22. Imágenes encontradas en el teléfono
Fuente: Propia

Videos: A través de esta adquisición fue posible recuperar 2 videos del teléfono celular. El primer video llamado 03102008031.mp4 se encontró en la ruta C:\Data\Videos\200810\200810A0\. El segundo video corresponde al archivo llamado CONDONES.3gp, ubicado en C:\Data\Videos\. Este ultimo archivo, debido a que no responde a ningún patrón de nombre como el primer video hallado, y a que tampoco se encuentra indexado automáticamente por el sistema operativo del teléfono celular, se puede llegar a pensar que proviene de una fuente externa al teléfono, y que no fue capturado por originalmente por este teléfono.

A continuación se muestran las propiedades de cada uno de los videos hallados en la adquisición:

Video # 1: 03102008031.mp4

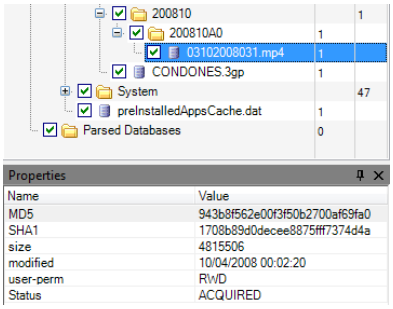


Figura 4. 23. Datos del primer video encontrado en el dispositivo
Fuente: Propia

Video # 2: CONDONES.3gp

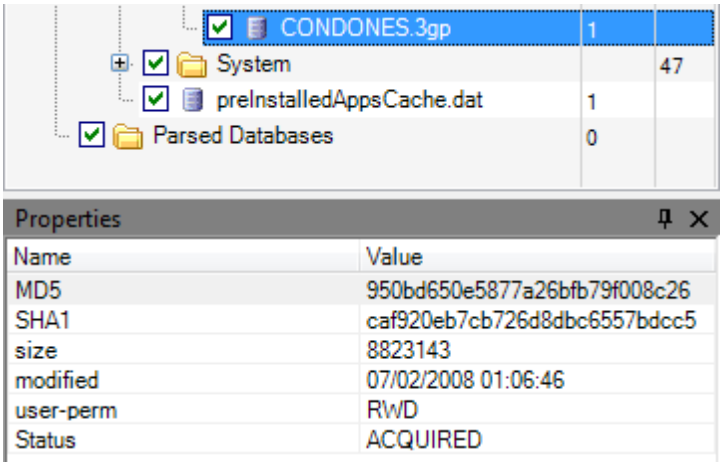


Figura 4. 24. Datos del segundo video encontrado en el dispositivo
Fuente: Propia

Audio: A través de esta adquisición fue posible recuperar 6 archivos de audio digital del teléfono celular vulnerado. Todos los archivos se encontraron en la ruta C:\Data\Sounds\Digital\. Entre los archivos se encuentran 5 archivos en formato mp3, y 1 archivo en formato amr. De los 5 archivos en formato mp3, 4 de ellos presentan información ID3 que indican tanto nombre del archivo como el autor, haciendo pensar que se trata de archivos de música. El listado de archivos de audio es el siguiente:

- 05 de que te las picas(2).mp3
- 16se la robe y me la robaron38.mp3
- 36 1que de raro tiene.mp3
- Celia Cruz – Yo vivire (Sobrevivire).mp3
- Clip de sonido.amr
- con la tierra encima.mp3

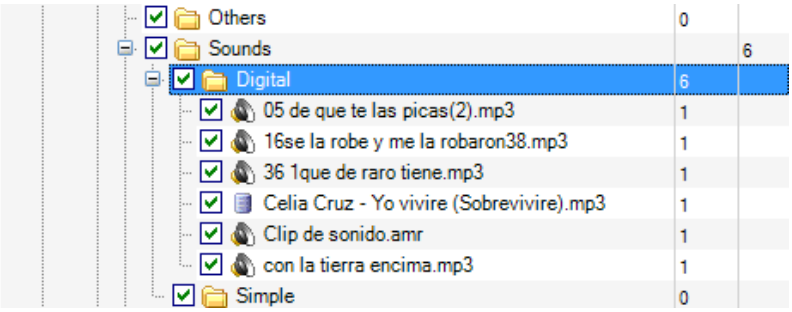


Figura 4. 25. Archivos de audio encontrados en el dispositivo
Fuente: Propia

Mensajes multimedia: No se obtuvo información relevante relacionada con mensajes multimedia en esta adquisición.

Mensajería instantánea y navegación web: No se obtuvo información relevante relacionada a mensajería instantánea multimedia en esta adquisición.

Documentos electrónicos: No se obtuvo información relevante relacionada documentos electrónicos en esta adquisición.

Identificar procesos en ejecución: No se obtuvo información relevante relacionada procesos en ejecución en esta adquisición.

Revisar los logs del sistema (dependen del sistema operativo): A través de la adquisición del sistema de archivos, se logró obtener una serie de registros de instalación de aplicaciones externas en el sistema.

FASE DE ANÁLISIS

Las aplicaciones que se encontraron fueron las siguientes:

Nombre de la Aplicación	**Ruta de Instalación**	**Nombre del ejecutable**	**Fecha y Hora de Instalación**
Bloover	C:\private\10203366\midlets\[100ff9d8]\	Blooover2.jar	09/04/2010 04:24:30
iSexPlayer	C:\private\102033e6\midlets\[10136200]\	iSexPlayer	09/04/2010 23:25:46
SuperBluetooth Hack	C:\private\102033e6\midlets\[101747e1]\	SuperBluetooth Hack v1.07.jar	09/04/2010 04:20:06
EA Mobile Burnout	C:\private\102033e6\midlets\[10143608]\	ea Mobile Burnout	08/18/2010 03:00:12
Turbo Jet Ski 3D	C:\private\102033e6\midlets\[10132c1e]\	turbo Jet Ski 3D s60v3 240x320.jar	08/18/2010 03:07:38
MagicBlueHack	C:\private\102033e6\midlets\[101301b6]\	magicBlueHack.jar	10/07/2010 03:13:24
Dtm Race Driver 3	C:\private\102033e6\midlets\[1012479d]\	dtm Race Driver 3d.jar	08/18/2010 03:20:20

Tabla 3. Log de instalación de aplicaciones

Fuente: Propia

Sin embargo, a través de esta adquisición, no fue posible obtener la carpeta private ni ninguna de sus subcarpetas, por lo cual no fue posible acceder ni obtener ninguno de los programas hallados en las rutas especificadas por los registros de instalación de aplicaciones externas.

Identificar rastros de conexiones (Bluetooth, irda, cable): No fue posible determinar información referente a algún tipo de conexión de algún tipo con otro dispositivo en esta adquisición.

Análisis de los archivos obtenidos (correlación de eventos):

Fecha Inicio	Fecha Fin	Acción	Registros Eliminados	Número de la llamada
07/10/2011 3:13:24	07/10/2011 3:13:24	Instalación de la aplicación MagicBlueHack	N/A	N/A
04/09/2011 4:20:06	04/09/2011 4:20:06	Instalación de la aplicación SuperBluetoothHack	N/A	N/A
24/09/2011 23:25:46	24/09/2011 23:25:46	Instalación de la aplicación iSexPlayer	N/A	N/A
04/09/2011 4:24:30	04/09/2011 4:24:30	Instalación de la aplicación Bloover	N/A	N/A
04/09/2011 4:23:07	04/09/2011 4:23:07	Cambio del lenguaje de la aplicación ejecutada	N/A	N/A
21/10/2011 22:45	21/10/2011 22:57	Eliminación de registro de eventos	29	*300
22/10/2011 18:23	22/10/2011 18:24	Eliminación de registro de eventos	4	72400256
22/10/2011 20:51:36	22/10/2011 20:51:44	Eliminación de registro de eventos	2	76160055
22/10/2011 21:43:49	22/10/2011 21:45:49	Eliminación de registro de eventos	7	70452361
22/10/2011 21:58:29	22/10/2011 21:58:33	Eliminación de registro de eventos	2	72452369

Tabla 4. Correlación de eventos

Fuente: Propia

FASE DE ANÁLISIS
En la anterior tabla se puede observar los eventos más relevantes detectados durante el análisis. Una relación importante es que el mismo día en que se instaló la aplicación SuperBluetoothHack (04/09/11) a los tres minutos se eliminó una entrada en la tabla de lenguaje por defecto permitiendo cambiar momentáneamente el lenguaje de la aplicación ejecutada, que en este caso es SuperBluetoothHack. Otra relación que se establece es que luego de instalar la aplicación isexplayer (la cual está considerada como el primer virus para sistemas Symbian S60 tercera edición) aparecen registros de eliminación de logs de llamadas a números extraños como *300 y de otros aleatorios. Los intervalos de tiempo son tan cortos que se establece que es muy posible que sean realizados automáticamente por el mismo sistema o por un programa automatizado corriendo por debajo.
Resumen: Se obtuvo la información necesaria para poder trabajar correctamente con el dispositivo, esto es, se identifico el modelo, y de esta manera, sus características técnicas principales. Además se identificaron las posibles fuentes de evidencia, se realizó la recolección y preservación de datos mediante las herramientas forenses, aplicaciones del fabricante y se recurrió a las fotografías digitales para aquellos que no pudieron extraerse mediante éstas aplicaciones.
Documento/Archivos Digitales: Manuales digitales, aplicaciones del fabricante, imágenes digitales. Archivos de audio(mp3). Registro de llamadas. Reportes sobre la evidencia extraída.

REPORTE
Los reportes de hallazgos son generados por la herramienta seleccionada, en este caso Device Seizure, en distintos formatos dependiendo de la selección del investigador forense.
Resumen: Se realizaron dos actividades fundamentales: a) Reporte de Resultados y b) Revisión de la metodología.

4.3. Análisis de Resultados

La presente sección expone las conclusiones del caso a las cuales se llegaron después de realizar la revisión de la metodología:

- ✓ Basados en las figuras se concluye que el análisis forense de las dos adquisiciones se realizaron sobre el mismo dispositivo de fabricante Nokia, modelo RM-132.
- ✓ Se concluye que, entre el 21 y 22 de octubre de 2011 se eliminaron en total 45 registros de eventos en el dispositivo los cuales, en su gran mayoría, se realizaron con pocos segundos o minutos de diferencia eliminando registros de llamadas al *300 (número de servicio al cliente del operador TIGO) por lo que este proceso fue realizado por un programa malicioso automatizado.
- ✓ El día 4 de septiembre de 2011 se realizó un cambio de lenguaje de una aplicación el cual no quedó en los registros del dispositivo debido a que fue deliberadamente eliminado, siendo recuperado por la herramienta de adquisición.
    - El día 22 de octubre de 2011 se eliminaron 8 registros de llamadas tanto perdidas como recibidas y realizadas. Se destaca un registro eliminado del número 000000 que tuvo una duración de 00:00:00 y fue realizado a las 11:20:09 el cual fue realizado por un programa automatizado enmascarando otro registro de llamada a otro destino y con otra duración (¿Métodos anti-forenses en teléfonos celulares?).

- ✓ La lista de contactos obtenida en la adquisición corresponde con la del usuario, es decir, no se eliminó, modificó o agregó ningún contacto.
- ✓ El calendario del dispositivo no tuvo modificaciones.
- ✓ Se detectó la instalación de la aplicación iSexPlayer la cual se considera el primer malware para dispositivos Symbian OS tercera edición. Dicha instalación fue corroborada por el dueño del dispositivo, sin embargo, comenta que le llegó como un mensaje sin que él tuviera que confirmar por lo que se concluye que fue enviada utilizando suplantación de un dispositivo de confianza.
- ✓ Se encontró un archivo sospechoso el cual especifica una ruta en la que se encuentra archivos confidenciales como la lista de contactos entre otros, sin embargo, este texto hace parte de una herramienta de auditoria instalada y ejecutada la cual se llama Bloover2 y su finalidad es realizar auditoria de ataques Bluetooth conocidos como Bluesnarfer por lo cual se concluye que dicha evidencia no representa ningún ataque realizado en el dispositivo en cuestión.
- ✓ Se encontraron varios rastros de conexiones y sincronizaciones utilizando la herramienta PC Suite del fabricante Nokia las cuales fueron corroboradas por el usuario por lo que se concluye que no constituyen evidencias digitales de ataques realizados al dispositivo.
- ✓ Al realizar la búsqueda de las direcciones MAC de los dispositivos incautados se encontró un texto el cual representa un rastro de una conexión Bluetooth por lo cual, teniendo en cuenta que el dongle USB Bluetooth y el otro teléfono celular incautado tenían la misma MAC, se concluye que se realizó una conexión Bluetooth suplantando un dispositivo de confianza.
- ✓ Se encontraron las fechas y horas de instalación de las diferentes aplicaciones que residen en el dispositivo destacando que virus iSexPlayer fue instalado el 24 de septiembre de 2011 por lo cual se concluye que esta aplicación es la responsable de realizar la eliminación del registro con número de destino 000000, una duración de 00:00:00 y fecha de realización a las 11:20:09.

- ✓ Una relación importante es que el mismo día en que se instaló la aplicación SuperBluetoothHack (04/09/11) a los tres minutos se eliminó una entrada en la tabla de lenguaje por defecto permitiendo cambiar momentáneamente el lenguaje de la aplicación ejecutada, que en este caso es SuperBluetoothHack.

CONCLUSIONES

El campo de la informática forense tiene aún muchas áreas por investigar, una de ellas es la de los dispositivos móviles, en este sentido es que en el presente trabajo de investigación se realizo una extensa investigación acerca de la informática forense clásica como en dispositivos móviles, esto se llevo a cabo con el fin de realizar la propuesta metodología de recolección de evidencia digital en dispositivos móviles (celulares GSM). A partir de la investigación realizada es importante tomar en cuenta algunos puntos, estos se describen a continuación:

• Existe un área de exploración importante en el campo de la informática forense orientada a dispositivos móviles, pues esta rama de las ciencias forenses esta en surgimiento, y requiere de aportes continuos y más investigación.

• Fue fundamental el realizar una extensa adquisición de material bibliográfico, puesto que le dio bases serias a la investigación, y permitió avanzar rápidamente a través de los capítulos propuestos para finalmente proponer una metodología.

• Al final del proceso de ejecución de la metodología, se pudo concluir que es viable llevar a cabo su aplicación, teniendo en cuenta los puntos expuestos en el capítulo del análisis de resultados.

RECOMENDACIONES

- El campo de seguridad informática en dispositivos móviles está actualmente creciendo debido a que cada vez los dispositivos son más complejos e incluso son capaces de realizar transacciones a través de *web services* lo cual conlleva a riesgos de seguridad en cuanto a transacciones bancarias entre otros. Se recomienda investigar sobre la metodología enfocada a seguridad en *web services*

- Se propone desarrollar procesos metodológicos para la investigación de incidentes en dispositivos móviles de otro tipo de tecnologías diferentes a GSM, como lo es 3.xG u otro tipo de conexiones como es Wi-fi o Wi-Max debido a que es más probable explotar vulnerabilidades en el dispositivo, además que cada vez se encuentra más cantidad de información crítica y es más fácil acceder al dispositivo de forma inalámbrica y sin interacción.

- Teniendo en cuenta el gran éxito que ha tenido el iPhone 3G a nivel mundial, se propone investigar en el diseño, e implementación y validación de una metodología orientada a incidentes en este tipo de dispositivo.

BIBLIOGRAFÍA

ALZAROUNI, M. *Mobile Handset Forensic Evidence: a challenge for Law Enforcement*. Noviembre de 2007.

AYERS R. ;JANSEN W.. *Guidelines on CellPhone Forensics*, National Institute of Standards and Technology Special Publication 800-101;[http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf]. Última consulta: Diciembre de 2011.

B. RAYNER. *"Mobile Phone Security".* East Carolina University [http://www.infosecwrite rs.com/text_resources/pdf/Phones_BRayner.pdf)]. Última visita Noviembre de 2011.

CARPENTER, P. *The Emerging Mobile Malware Threat*. Noviembre 18 de 2006. [http://securityhrenaissance.com/wordpress//wordpress/wp-content/uploads/2007/01/mob ilemalware.pdf.] Última consulta: Diciembre de 2011.

CÓDIGO PENAL, (Bolivia) Art. 363, 362

CONSTITUCIÓN POLÍTICA DEL ESTADO PLURINACIONAL DE BOLIVIA, Art. 133, 134

CSI. *Computer Crime and Security Survey* .[http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf.], Última consulta: Octubre de 2011.

D. HOFFMAN. *Blackjacking* . Wiley Publishing. Indianapolis, United States of America. 2007. Última visita Noviembre de 2011.

INFOPLEASE *Cell Phone Usage Worldwide, by Country*. [http://www.infoplease.com/ipa/A0933605.html.] Última consulta: Noviembre de 2011.

INFOBAE. *Nokia y Samsung le quitan porción de mercado a Motorola*. 23 de Abril de 2007. [http://tecnologia.infobaeprofesional.com/notas/44978-Nokia-y-Samsung-le-quitan-porcion-de-mercado-a-Motorola.html?cookie.] Última consulta: Noviembre 2011.

LEY 26388 (Argentina) Promulgada el 24 de junio de 2008

LEY 19223 (Chile) Promulgada en 1993.

LEY 1273 (Colombia) del 5 d enero de 2009

LEY 164 (Bolivia) Promulgada el 8 de agosto de 2011.

LIMA MARIA DE LA LUZ. *Delitos Informáticos.* Última consulta Diciembre de 2011.

LÓPEZ O.,AMAYA H.;LEÓN R.;ACOSTA B. *Informática forense: Generalidades, aspectos técnicos y herramientas*. Universidad de los Andes (2002). Bogotá, Colombia. [http://w ww.criptored.upm.es/guiateoria/gt_m180b.htm]. Última consulta: Diciembre de 2011.

MELLAR, B. *Forensic examination of mobile phones.* Noviembre de 2007.

MOBILE USER EXPERIENCE. *What happened to handset industry margins in Q307?*. [http://www.pmn.co.uk/images/q307marginsm.JPG.] Última consulta: noviembre de 2011.

PEISERT S.; BISHOP M.KARIN S.;MARZULLO K. *Toward Models for Forensic Analysis*. In Proceedings of the Second International International Workshopon Systematic approaches to digital forensic engineering (SADFE'07), 2007. Última consulta Noviembre de 2011.

POLLITT M. *Computer Forensics: an Approach to Evidence in Cyberspace*, Proceedings (Vol. II, pp 487-491) of the National Information Systems Security Conference, Baltimore, MD. 1995 [http://www.digitalevidencepro.com/Resources/Approach.pdf]. Última consulta: Noviembre de 2011.

SARZANA CARLOS, *Criminalitá e Tecnología*. Última consulta Diciembre de 2011.

SOSA MONTIEL. *Delitos Informáticos.* Última consulta Diciembre de 2011.

THE GLOBALIST, SYNDICATION SERVICES. *Cell Phones and Globalization*. [http://www.theglobalist.com/globalicons/syndication/sample.htm.] Última consulta: Noviembre de 2011.

TELLEZ V. JULIO. *Derecho Informático.* Última consulta Diciembre de 2011.

ANEXO N° 1

1. Ud. ha escuchado hablar de la Informática Forense

SI ☐

NO ☐

2. Conoce el objetivo de la Informática Forense

SI ☐

NO ☐

3. Durante el desarrollo de sus actividades profesionales a aplicado alguna técnica forense ☐

SI

NO ☐

4. Conoce de casos ilícitos en los que se ha visto involucrado un dispositivo móvil (teléfono celular GSM)

SI ☐

NO ☐

5. Conoce de herramientas para la recolección de evidencia digital

SI ☐

NO ☐

6. Considera de importancia contar con herramientas (metodologías) que ayuden al esclarecimiento de casos ilícitos en los que se vea involucrada la tecnología

SI ☐

NO ☐

7. Conoce de normas bolivianas que penalizan los delitos informáticos

SI ☐

NO ☐

Cual……
……

ANEXO N ° 2

ENTREVISTA AL PROPIETARIO DEL DISPOSITIVO

1. Desde cuando es propietario del dispositivo?

2. Lo compro nuevo o usado?

3. Usualmente que uso le da a su teléfono celular?

4. Utiliza frecuentemente la tecnología Bluetooth?

5. Sincroniza el contenido de su teléfono con algún computador en especial. Cómo realiza este procedimiento?

6. Además de las conexiones con las manos libres, ¿Ha utilizado últimamente Bluetooth con algún otro dispositivo?

7. ¿Dentro de los últimos días alguien más ha tenido acceso a sus manos libres?

8. ¿Ha notado la ausencia de algún tipo de información (fotos, videos, mensajes, contactos, documentos) que se encontraba almacenada en su teléfono celular?

9. ¿Realiza alguna otra conexión con su teléfono celular distinta a las ya mencionadas?

ANEXO N° 3

LISTA DE CHEQUEO PARA SELECCIÓN DE HERRAMIENTAS FORENSES EN DISPOSITIVOS MÓVILES GSM

Nombre de la herramienta:

Versión:

ITEMS OBLIGATORIOS	***CUMPLE***	***NO CUMPLE***
Es una herramienta de solo lectura?		
Soporta el dispositivo?		
Realiza adquisición física?		

ITEMS PRIMER GRADO	***CUMPLE***	***NO CUMPLE***
Permite búsqueda de palabras claves?		
Realiza verificación de integridad de archivos?		
Proporciona frecuentemente actualizaciones y soporte técnico?		

ITEMS SEGUNDO GRADO	***CUMPLE***	***NO CUMPLE***
Soporta visor hexadecimal?		
Realiza DataCarving?		
Recupera Información Borrada?		
Permite generar reportes en formato estándar? XML, DOC,PDF.		