ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMATICA Y ELECTRONICA

INGENIERIA EN SISTEMAS

TEMA:

"ESTUDIO Y APLICACIÓN DE PROCEDIMIENTOS DE ANÁLISIS FORENSE EN SERVIDORES DE BASES DE DATOS SQL SERVER Y MYSQL, CASO PRÁCTICO: DESITEL - ESPOCH**"**

TESIS DE GRADO

Previa obtención del Título de

INGENIERO EN SISTEMAS INFORMÁTICOS

PRESENTADO POR:

Ana Lucía Juntamay Tenezaca

Nancy Patricia Macas Carrasco

RIOBAMBA – ECUADOR

2011

AGRADECIMIENTO

Nuestro más sincero agradecimiento a Dios por bendecirnos, ser nuestro guia y compañero en todo momento.

A nuestra querida institucion ESPOCH por permitirnos crecer intelectual y profesionalmente.

A nuestra directora de tesis , Ingeniera Gloria Arcos por su tiempo, confianza, paciencia, consejos y apoyo durante el desarrollo de la tesis.

Al presidente del tribunal de nuestra tesis, Ingeniero Diego Ávila por su tiempo, atención y sugerencias durante la revisión de esta tesis.

A todos los que contribuyeron de una u otra forma apoyándonos desinteresadamente durante el desarrollo de esta tesis de grado.

DEDICATORIA

Con mucho cariño a mis padres, pilares fundamentales en mi vida. Gracias por todo papá y mamá por darme una carrera para mi futuro y por creer en mí.

A mis hermanas por estar conmigo y apoyarme siempre.

También dedico este proyecto a mi esposo Gustavo, por su paciencia, por su comprensión, por su fuerza, por su amor, por ser tal como es.

A mí querida hija Mishell, incentivo para cumplir mis metas y anhelos, y quien es la alegría en mi vida.

Nancy Patricia Macas Carrasco

Dedico este trabajo de tesis con todo mi corazón, admiración y respeto:

A mi Madre porque no existen palabras que puedan expresar su amor incondicional, a mi padre por los sacrificios realizados para darme una carrera profesional.

A mis Hermanas y mi hermano por su cariño y amor fraternal.

A Dios por existir, por su amor y cuidar de mí y mi familia de manera irrevocable e incondicional.

Ana Lucía Juntamay Tenezaca

FIRMAS DE RESPONSABILIDADES

NOMBRE	**FIRMA**	**FECHA**
Ing. Iván Menes **DECANO DE LA FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**	**……**	**……**
Ing. Raúl Rosero **DIRECTOR DE ESCUELA DE INGENIERÍA EN SISTEMAS**	……	……
Ing. Gloria Arcos **DIRECTORA DE TESIS**	**……**	**……**
Ing. Diego Ávila **MIEMBRO DEL TRIBUNAL**	**……**	**……**
Tlgo. Carlos Rodríguez **DIRECTOR DPTO. DOCUMENTACIÓN**	**……**	**……**
NOTA DE LA TESIS	**……**	

“Nosotras, ANA LUCÍA JUNTAMAY TENEZACA Y NANCY PATRICIA MACAS CARRASCO somos responsables de las ideas, doctrinas y resultados expuestos en esta tesis; y, el patrimonio intelectual de la Tesis de Grado pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO”.

Ana Lucía JuntamayTenezaca

Nancy Patricia Macas Carrasco

ÍNDICE DE ABREVIATURAS

ASP	Active Server Pages
BD	Base de Datos
CFFTPM	Cyber Forensic Field Triage Process Model
CGI	Common Gateway Interface (Interfaz de Entrada Común)
CRM	CustomerRelationship Management(Gestión de Relación con los Consumidores)
DBA	Data Base Administrador(Administrador de Base de Datos)
DBMS	Data Base Management System(Sistemas de Gestión de Bases de Datos)
DCSA	Análisis Digital de Escena del Crimen(Digital Analysis of CrimeScene)
DFRW	Digital ForensicResearch Workshops(Investigación Forense Digital de Talleres)
DLL	Dynamic Linking Library (Librería de Enlace Dinámico)
DML	Data Manipulation Language (Lenguaje de Manipulación de Datos)
DOM	Document Object Model(Modelo de Objetos de Documento)
ERP	Enterprise Resourse Planning (Planificación de Recursos Empresariales)
FAT	File Allocation Table (Tabla de Ubicación de Ficheros)
IDS	Intrusion Detection System(Sistema de Detección de Intrusos)
IP	Internet Protocol(Protocolo de Internet)
IPS	Intrusion Prevention System (Sistema de Prevención de Intrusos)
ISECOM	Institutefor Security and Open Methodologies (Instituto para la

	Seguridad y Metodologías Abierto)
ISSAF	Information Systems Security Assessment Framework(Sistemas de Información de Seguridad Marco de Evaluación)
MAC	Media Access Control (Control de Acceso al Medio)
MD5	Message-DigestAlgorithm 5(Algoritmo de Resumen del Mensaje 5)
MDAC	Microsoft Data Access Client (Acceso a Datos al Cliente Microsoft)
MYD	MYData (My Datos)
MYI	MYIndex (My Índices)
NIST	Instituto Nacional de Estándares y Tecnologías
NTFS	New Technology File System (Nuevo Tecnología de Sistema de Archivo)
ODBC	Open DataBase Connectivity(Conectividad Abierta de Bases de Datos)
OISSG	Open Information System Security Group (Sistema Abierto de Información de Grupo de Seguridad)
OLAP	On-Line Analytical Processing (Procesamiento Analítico en Línea)
OLTP	OnLine Transaction Processing (Procesamiento de Transacciones en Línea)
OSSTMM	Open Source Security Testing Methodology Manual (Manual de la Metodología Abierta de Testeo de Seguridad)
PHP	Hypertext Pre-processor (Hypertext Pre-Procesador)
RAM	Random Access Memory (Memoria de Acceso Aleatorio)
RTO	Objetivo De Tiempo De Recuperación (Recovery Time Objective)
SGBD	Data Base Management System (Sistema de Gestión de Bases de Datos)

SPID	Process Server Identified (Proceso del Servidor Identificado)
SQL	Lenguaje De Consulta Estructurado (Structured Query Language)
URL	Uniform Resource Locator (Localizador Uniforme de Recursos)
XML	eXtensible Markup Language (Lenguaje de Marcas Extensible)
XSS	Cross-SiteSripting

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad, la mayoría de las instituciones manejan la información en forma digital por lo que es de suma importancia contar con la capacidad para buscar, recolectar y preservar datos electrónicos en una forma eficiente en tiempo y costo, y con validez legal, entre ellos podemos citar algunas necesidades comunes son: Investigaciones de fraude internas y externas, auditorias de información, actividades Maliciosas, asuntos de Recursos Humanos, Robo de Propiedad, delitos cibernéticos entre otros.

La tecnología ha tenido un desarrollo sorprendente en los últimos años, tanto así que ahora es utilizada para cometer delitos informáticos tales como: clonación de tarjetas, piratería, sustracción de datos, modificación de datos, entre otros, algunos de estos delitos no están tipificados en la legislación, lo que impide el accionar de las instituciones judiciales.

.

La problemática antes mencionada hace surgir la necesidad de aplicar la informática forense, como medio que ayude a esclarecer hechos delictivos informáticos, contar con una guía de procedimientos de análisis forense para detectar las vulnerabilidades de base de datos y aplicarlos de forma adecuada haciendo uso de herramientas software posibilita recolectar y o recopilar información valiosa para la institución.

La guía de procedimientos de análisis forense se encuentra conformada por las fases de: Identificación, Verificación, Recolección de evidencias, Análisis de evidencias, Recuperación de datos y Preparación de informe, estas fases se basan en modelos estándares y procedimientos más aceptados en cuanto a informática forense. Se debe seguir la guía paso a paso de forma que sea aceptada en cualquier proceso legal

Existe una variedad de herramientas software para trabajar en el análisis de vulnerabilidades, recuperación y análisis forense en base de datos tales como: Acunextix Vulnerability Web, NGSSQuirrel, Aronis Recovery for SQL Server, Stellar Phoenix for MySQL y Windows Forensic ToolChest.

En cuanto a fuentes de información se utilizaron principalmente aquellas que se refieren al tema de investigación como libros, revistas, páginas web similares, etc casi como la observación, para la elaboración y aplicación de la guía se realizaron entrevistas a los Técnicos que la trabajan dentro de la institución para determinar las necesidades que se deben cubrir.

El presente estudio se aplico en la ciudad de Riobamba, en la Escuela Superior Politécnica de Chimborazo, Departamento de Sistemas y Telemática(DESITEL). el documento se encuentra estructurado en las siguientes capítulos: MARCO REFERENCIAL, en el cual se da a conocer el ámbito de la tesis con sus antecedentes, objetivos, justificación y la comprobación de la hipótesis: MARCO TEÓRICO en el cual se plasma el estudio en el análisis forense y una introducción a las bases de datos y la seguridad; MODELOS DE ANÁLISIS FORENSES en la cual se hace una revisión de los diferentes modelos de análisis forenses; ESTUDIO DE HERRAMIENTAS SOFTWARE en este capítulo se estudio las diferentes herramientas de: vulnerabilidad, recuperación y reparación y análisis forense de base de datos; PROPUESTA DE LA GUIA DE TÉCNICAS Y PROCEDIMIENTOS DE ANALISIS FORENSE EN UNA BASE DE DATOS en la cual se estudia diferentes procedimientos de análisis forense, alcances, limitaciones, característica y fases de la guía propuesta y APLICACIÓN DE LA GUIA DE PROCEDIMIENTOS DE ANALISIS FORENSE EXPUESTOS EN DESITEL-ESPOCH en la cual se empleo la guía de procedimientos propuesta en escenarios reales.

CAPÍTULO I

MARCO REFERENCIAL

1.1. ANTECEDENTES

Hoy en día, se hace impensable administrar un negocio cualquiera sea su envergadura, sin la implementación de algún tipo de software de base de datos. Sistemas de Recursos Humanos, Liquidación de Haberes, Administración de Clientes,ERPs, CRMs, Aplicaciones Web interactivas, son tan solo algunos de los sistemas que a menudo suelen ser requeridos en gran parte de los escenarios de negocio, los mismos que requieren indirectamente un gestor de base de datos.

El activo más valioso que una empresa posee es la Bases de datos, sin embargo, se presta muy poca atención en la obtención y registro de las transacciones. Además, en un esfuerzo para reducir costos, muchas organizaciones están consolidando varias bases de datos en los sistemas de misión crítica, que son frecuentemente blanco de los atacantes.

Un problema que hoy en día se presenta frecuentemente es que el administrador de seguridad de bases de datos, si es el caso, no tiene claro un procedimiento sencillo y eficaz para manejar los incidentes en una base de datos. Esto se debe en gran medida a

la inexistencia de capacitación en informática forense, por ello la falta de personal capacitado para llevar un caso de evidencia digital o análisis forense.

Actualmente, en bases de datos encontramos un problema al intentar administrar evidencia digital, debido a que es difícil definir, producir, obtener y analizar la evidencia e implica un mayor esfuerzo aplicar análisis forense, debido a que este tema no ha sido tratado profundamente, y menos aún en bases de datos.

Los principios de la Informática forense pueden aplicarse a una base de datos, que es un almacén de datos persistente, a menudo relacional. Por ejemplo, las marcas de tiempo que se aplican a la hora de actualizar una fila de una tabla relacional pueden ser inspeccionadas y probadas para su validez a fin de verificar las acciones de un usuario de base de datos.

Con la llegada de nuevas tecnologías, su utilización y adopción por gran cantidad de personas, surgen amenazas y es por ello que es importante hablar de la seguridad en cuanto a bases de datos. La seguridad de la información y de los sistemas, es un punto crítico en una sociedad en la que la información digital se considera como un bien o activo valioso al cual se debe proteger.

Las corporaciones están adaptando políticas internas de seguridad para contemplar la preservación de evidencia informática y estar preparados para delitos electrónicos. La Informática Forense resulta de utilidad para ayudar en la obtención y preservación de evidencia y su posterior análisis forense informático.

El trabajo de investigación realizará la revisión de la informática forense describiendo el contexto general de la disciplina en la actualidad, para luego explicar los modelos de investigación existentes que ayudan a realizar un análisis forense adecuado. Se expondrán una serie de modelos de investigación en el área de informática forense, a fin de proporcionar un mejor entendimiento de los procedimientos y estándares actuales de la informática forense en el mundo. Entre los modelos revisados que tienen mayor importancia citamos los siguientes: Modelo Digital Forensic Research

Workshops(DFRW), Modelo Forense Digital Abstracto y Modelo propuesto por NIST, en realidad existen diversos tipos de modelos investigativos que han sido propuestos a través de los años, los cuales permiten entender los procedimientos y estándares definidos en la actualidad para realizar una investigación forense.

Es necesario mencionar que hoy en día en el mercado existen diferentes herramientas forenses que ayudan a realizar análisis forense facilitando así el proceso investigativo de tal forma que refleje los resultados deseados por los analistas. Las herramientas software se enfocan en diferentes áreas como análisis forense de redes, sistemas de archivos, para nuestro estudio se analizarán las Herramientas Forenses que se pueden aplicar a Bases de Datos como son: SQL Server Management Studio Express, SQLCMD, Windows ForensicToolchest, DD\DCFLDD, MD5SUM, NetCat/Cryptcat, WinHex, EnCase y otras que se detallarán durante la investigación. Algunas de estas herramientas son pagadas y otras libres, cada una de ellas poseen características y funcionalidades diferentes, las cuales serán utilizadas para el desarrollo de la guía de referencia propuesta.

El presente estudio se encontrará enfocado a una investigación de los procedimientos y técnicas de análisis forense aplicado al Sistema Manejador de Bases de Datos SQL Server y MySQL, a fin de proponer, aplicar y evaluar una guía para realizar análisis forenses orientados a incidentes Servidores de Bases de Datos del Sistema Académico de la ESPOCH.

1.2. JUSTIFICACIÓN DEL PROYECTO DE TESIS

Para sustentar la razón, importancia y visión de la presentación del anteproyecto de tesis, establecemos tres tipos de justificación: El elemento teórico encaminado al aporte investigativo, la justificación metodológica en la que se explica la necesidad de desarrollar una guía de referencia de análisis forense en bases de datos SQL Server. Y la justificación aplicativa correspondiente a la descripción de la aplicación práctica.

1.2.1. JUSTIFICACIÓN TEÓRICA

Las Bases de Datos incluidas hoy en día en los sistemas de información de cualquier organización, nacen con el fin de resolver las limitaciones que en algunos casos presentan los ficheros para el almacenamiento de información. En los entornos de Bases de Datos, las diferentes aplicaciones y usuarios utilizan un único conjunto de datos integrado a través de un Sistema de Gestión de Bases de Datos (SGBD).
Por otra parte, la agrupación de datos pertenecientes a distintos usuarios y catalogados en niveles de seguridad diferentes aumenta los riesgos en cuanto a la seguridad de los datos. Sin lugar a dudas el motivo más importante por el cual las bases de datos suelen ser vulnerables a algunos de los ataques, se encuentra íntimamente relacionado con la poca importancia que por “extraños motivos” las empresas brindan a sus almacenes de datos.

Para investigar ataques a sistemas informáticos apareció la Informática Forense, aunque hoy en día las investigaciones forenses tradicionales frecuentemente excluyen la base de datos, puesto que se centran en descubrir incidentes en el sistema operativo y en la red de datos. Sin embargo el análisis forense en Bases de Datos permite identificar datos de pre y post transacción, puede ayudar a demostrar brechas de seguridad de datos y recolectar evidencias infalibles.

1.2.2. JUSTIFICACIÓN METODOLÓGICA

La guía de referencia que se propone servirá para entender los numerosos aspectos que se relacionan con el proceso de un análisis forense en bases de datos, y permitirá realizar de forma adecuada y ordenada, obteniendo así un proceso investigativo consistente, estructurado y confiable. Cabe mencionar que para el adecuado desarrollo de la guía se estudiarán modelos de análisis forense que existen en la actualidad, las herramientas y procedimientos los cuales permiten que la investigación forense se realice con éxito sin pérdida o alteración de la potencial evidencia que pudiera llevarse a un proceso legal.

También se analizarán los problemas de seguridad que tiene un DBMS (Data Base Management System), debido a que sobre ellos vamos a realizar el análisis forense y es de vital importancia entender con claridad estos conceptos para conseguir una investigación adecuada y formal.

1.2.3. JUSTIFICACIÓN PRÁCTICA

No importa que tan seguro sea el firewall instalado en una empresa, si el personal no se encuentra capacitado, debilidades del factor humano por ejemplo, podrán suplir la falta de alguna vulnerabilidad explotable en sus sistemas de defensa. Por último, el administrador de base de datos, probablemente se encuentre preocupado porque la performance sea la correcta a la hora de servir datos a la aplicación web demandante, pero no se encuentra preparado para enfrentar un caso de investigación forense en una base de datos, como enfrentar este escenario, las medidas que deberá tomar y los procedimientos para recolectar evidencias.

La ESPOCH al igual que cualquier otra institución cuenta con aplicaciones web las mismas que interactúan con un Servidor de Base de Datos y que se encuentran expuestos a ataques externos o internos, o incluso a errores sin mala intención.
Nuestro trabajo de investigación consiste en proponer, aplicar y evaluar una guía metodológica para realizar análisis forenses en una base de datos. Esta investigación trata de dar respuesta a la pregunta: ¿Cómo desarrollar un análisis forense orientado a incidentes en base de datos? Para responder a este interrogante se realiza una revisión de los conceptos fundamentales, herramientas, modelos de investigación y procedimientos de la informática forense en general y su aplicación en base de datos.

De igual manera, se realizarán escenarios de pruebas en los que se aplicarán los ataques comunes en base de datos a fin de evaluar la guía propuesta, además se estudiará y aplicará herramientas de detección de vulnerabilidades a fin de mejorar la seguridad del servidor de base de datos La síntesis de los temas anteriores, provee una base y los conocimientos necesarios para presentar una guía metodológica, que luego será

probada, aplicada y analizada según sus resultados en el Servidor de Bases de Datos del Sistema Académico de la ESPOCH.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Desarrollar una guía de procedimientos de Análisis Forense para servidores de Bases de Datos SQL Server y MySQL, que será aplicada en el Departamento de Sistemas y Telemática de la ESPOCH.

1.3.2. OBJETIVOS ESPECÍFICOS:

- Revisar conceptos fundamentales, procedimientos de la informática forense en general y su aplicación en Servidores de Base de Datos, además conocer los problemas de seguridad que afectan a los Servidores de Base de Datos SQL Server y MySQL.
- Implementar escenarios de prueba donde se realicen los ataques más comunes a una base de datos.
- Realizar una copia de la base de datos del sistema académico a través de la red hacia la estación de trabajo forense, donde se utilizarán las herramientas de análisis forense que permitirán revisar y analizar los registros de las sentencias SQL ejecutadas, procesos, sesiones, permisos, etc.
- Analizar las principales herramientas de análisis forense aplicable a descubrir incidentes en Servidores de Bases de Datos SQL Server y MySQL.
- Estudiar los modelos de análisis forense más aceptados en esta disciplina en la actualidad, para entender de una mejor manera los procedimientos y estándares definidos para realizar una investigación forense.
- Aplicar la guía de referencia en la base de datos del Sistema Académico de la ESPOCH.

1.4. MARCO HIPOTÉTICO

1.4.1. HIPÓTESIS

La aplicación de la guía de técnicas y procedimientos de análisis forense permitirá obtener evidencias consistentes y facilitará la detección de vulnerabilidades.

1.5. MARCO METODOLÓGICO

1.5.1. MÉTODOS

Para la comprobación de la hipótesis será aplicado un método científico que permitirá establecer una secuencia ordenada de actividades que nos llevará a establecer nuestras conclusiones sobre la investigación realizada.
También se utilizará como complemento del presente trabajo al método, por cuanto, este establece el procedimiento necesario para la recopilación, análisis e integración de resultados necesarios para el desarrollo de la guía de técnicas y procedimientos de análisis forense en bases de datos.

1.5.2. TÉCNICAS

En Cuanto a fuentes de información se utilizará principalmente fuentes que se refieren al tema de investigación como páginas web, también se empleará la observación y experimentación por parte de los investigadores. Para la elaboración de la guía de procedimientos y técnicas, así como también del informe informático forense se realizará:

- Aplicación de Encuestas
- Elaboración de Entrevistas
- Revisión de Documentos
- Simulaciones
- Escenarios de Pruebas

CAPÍTULO II

MARCO TEÓRICO

2.1. ANÁLISIS FORENSE DIGITAL

Para realizar una guía de referencia que permita llevar a cabo análisis forense orientados a incidentes en el DBMS SQL Server o en MYSQL, es necesario entender principalmente la informática forense debido a que, es en ésta ciencia en donde se establecen los conceptos y procedimientos que permiten realizar la investigación. Se inicia con una revisión del contexto general de análisis forense digital, su propósito, los objetivos y algunas definiciones básicas del campo como las evidencias digitales y los aspectos legales que deben ser analizados.

2.1.1. Evidencia Digital

Una de las ideas principales del análisis forense, es poder realizar un estudio total de todo tipo de evidencia digital que se encuentre involucrada en un incidente (es decir, realizar recopilación, preservación, análisis y reportes de la evidencia), con el fin de hacer que esta evidencia cobre un valor legal, y que así mismo, sea admisible a la hora

de entablar procesos judiciales en los cuales esta evidencia tenga un carácter determinante en el mismo (17).

De acuerdo con el HB: 171 2003 Guide lines for the Management of IT Evidence, la evidencia digital es: "cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático".
Uno de los pasos a tener en cuenta en toda investigación, sea la que sea, consiste en la captura de la(s) evidencia(s). Por evidencia entendemos toda información que podamos procesar en un análisis. Por supuesto que el único fin del análisis de la(s) evidencia(s) es saber con la mayor exactitud qué fue lo que ocurrió. Podemos entender evidencia como (19):

- El último acceso a un fichero o aplicación (unidad de tiempo)
- Un Log en un fichero
- Una cookie en un disco duro
- El uptime de un sistema (Time to live o tiempo encendido)
- Un fichero en disco
- Un proceso en ejecución
- Archivos temporales
- Restos de instalación
- Un disco duro, pen-drive, etc.

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:

1. Es volátil
2. Es anónima
3. Es duplicable
4. Es alterable y modificable
5. Es eliminable

Estas características nos 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. Por tanto, es necesario mantener un conocimiento detallado de las normas y regulaciones legales asociadas con las pruebas y el derecho procesal, así como de las técnicas y procesos que permitan mantener la confiabilidad de los datos recogidos, la integridad de los medios, el análisis detallado de los datos y la presentación idónea de los resultados.

2.1.2. Delitos Informáticos

Los Delitos informáticos se encuentran en constante crecimiento convirtiéndose en un problema global para todas las empresas que utilizan Sistemas de Información y redes de comunicación como Intranet e Internet, una gran parte de las organizaciones tienen el pensamiento de que "Esto nunca nos ocurrirá a nosotros, si ocurre estamos bien preparados para enfrentarlo", no obstante este es un pensamiento erróneo porque el peligro de que sean víctimas de algún incidente o ataque está latente

Según Eugenio Urdaneta (11) un delito informático se puede definir como aquellas conductas ilícitas sancionadas por el ordenamiento jurídico, donde se hace uso indebido de las computadoras como medio o instrumento para la comisión de un delito, y así mismo aquellas otras conductas que van dirigidas en contra de las computadoras convirtiendo a éstas en su fin u objetivo.

Según Julio TellezValdes (12) conceptualiza al "delito Informático" en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

El presente trabajo considera el concepto del autor Julio TellezValdes, ya que define al delito informático de una forma simple y comprensible. Aunque no hay definición de carácter universal propia de delito Informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aun cuando no existe una

definición con carácter global, se han formulado conceptos utilizables atendiendo a realidades concretas.

Características

- Sólo una determinada cantidad de personas pueden llegar a cometerlos.
- El sujeto tiene cierto status socioeconómico y la comisión del delito no puede explicarse por pobreza, carencia de recursos, baja educación, poca inteligencia, ni por inestabilidad emocional.
- Son acciones ocupacionales, ya que generalmente se realizan cuando el sujeto atacado se encuentra trabajando.
- Son acciones de oportunidad, ya que se aprovecha una ocasión creada por el atacante.
- Provocan pérdidas económicas.
- Ofrecen posibilidades de tiempo y espacio.
- Son muchos los casos y pocas las denuncias.
- Presentan grandes dificultades para su comprobación, por su carácter técnico.
- Tienden a proliferar, por lo que se requiere su urgente regulación legal.

Clasificación de los Delitos Informáticos

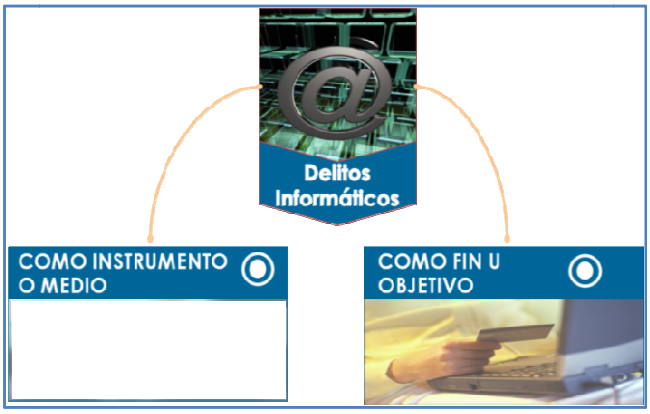


Figura II.1. Clasificación de Delitos Informáticos

Tipos de Delitos Informáticos existentes en la Legislación Ecuatoriana.

Los delitos que aquí se describen se encuentran como reforma al Código Penal por parte de la Ley de Comercio Electrónicos, Mensajes de Datos y Firmas Electrónicas publicada en Ley No. 67. Registro Oficial. Suplemento 557 de 17 de Abril del 2002.

Tabla II.I Tipos de Delitos

Tipo de Delito	Descripción
Delitos contra la Información Protegida: Violación de claves o sistemas de seguridad	Empleo de cualquier medio electrónico, informático o afín.
Delitos contra la Información Protegida: Destrucción o supresión de documentos, programas.	Destrucción o eliminación de Documentos, títulos, programas, datos, bases de datos, información, mensajes de datos contenidos anuncios del sistema o red electrónica.
Falsificación Electrónica	Utilice cualquier medio, altere, modifique mensaje de datos.
Daños Informáticos	Dolosamente, de cualquier modo o utilizando cualquier método destruya, altere, inutilice, suprima o dañe de forma temporal o definitiva: Programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica.
Fraude Informático	Utilización fraudulenta de sistemas de información o redes electrónicas con fines de lucro.
Violaciones al Derecho a la Intimidad	Violación al derecho a la Intimidad
Pornografía Infantil	Producción, comercialización y distribución de imágenes pornográficas de niños, niñas y adolescentes

Fuente: http://www.criptored.upm.es/guiateoria/gt_m592d.htm

2.1.3. ¿Qué es Análisis Forense Digital?

Existe una gran variedad de definiciones y conceptos para la interpretación y seguimiento adecuado del proceso de Análisis Forense Digital; sin embargo para nuestra investigación seleccionamos los siguientes:

Según Miguel López Delgado (3) Análisis Forense Digital es un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial.

Según WIKIPEDIA (7) el Análisis Forense Digital o examinación forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Los autores en cuanto se refiere a la definición de Análisis Forense Digital coinciden al señalar que se utilizan o son un conjunto de técnicas que consisten en algunos procedimientos que permitir obtener información que sea válida en un proceso legal. Las definiciones expuestas por los dos autores no difieren, sin embargo el segundo autor nos brinda un concepto más amplio que nos permite tener una mejor visión de dicho concepto.

Un incidente de seguridad informática puede considerarse como una violación o intento de violación de la política de seguridad, de la política de uso adecuado o de las buenas prácticas de utilización de los sistemas informáticos, como por ejemplo: Incidentes de denegación de servicios, de código malicioso, de acceso no autorizado, por uso inapropiado, incidente múltiple, etc.
Pero, ahora una vez ya ocurrido el incidente solo nos queda:

- Deducir que ha pasado.

- Qué ha motivado que esto haya pasado.
- Qué ha permitido llegar a ello.
- Qué acciones han sido consecuencia de ello.
- Qué podemos hacer para evitar que vuelva a suceder.

Principios forenses

Existen un gran número de principios básicos que son necesarios independientemente de si se está examinando un ordenador o un cadáver. Estos principios son (16):

- **Evitar la contaminación:** La esterilidad de los medios es una condición fundamental para el inicio de cualquier procedimiento forense en informática, pues al igual que en la medicina forense, un instrumental contaminado puede ser causa de una interpretación o análisis erróneo de las causas de la muerte del paciente.
- **Actuar metódicamente:**El investigador debe ser el custodio de su propio proceso, por tanto cada uno de los pasos realizados, las herramientas utilizadas (sus versiones, licencias y limitaciones), los resultados obtenidos del análisis de los datos, deben estar claramente documentados, de tal manera, que cualquier persona externa pueda validar y revisar los mismos. Ante una confrontación sobre la idoneidad del proceso, el tener documentado y validado cada uno de sus procesos ofrece una importante tranquilidad al investigador, pues siendo rigurosos en la aplicación del método científico es posible que un tercero reproduzca sus resultados utilizando la misma evidencia.
- **Controlar la cadena de evidencia, es decir, conocer quien, cuando y donde ha manipulado la evidencia:** Este punto es complemento del anterior. La custodia de todos los elementos allegados al caso y en poder del investigador, debe responder a una diligencia y formalidad especial es para documentar cada uno de los eventos que se han realizado con la evidencia en su poder. Quién la entregó, cuándo, en qué estado, cómo se ha transportado, quién ha tenido acceso a ella, cómo se ha efectuado su custodia, entre otras, son las preguntas que deben estar claramente resueltas para poder dar cuenta de la adecuada administración de las pruebas a su cargo.

2.1.4. Aspectos Legales

Desde abril del 2002 y luego de largas discusiones los honorables diputados aprobaron el texto definitivo de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, y en consecuencia las reformas al Código Penal que daban la luz a los llamados Delitos Informáticos.

Ahora bien el problema que se advierte por parte de las instituciones llamadas a perseguir las llamadas infracciones informáticas es la falta de preparación en el orden técnico tanto de la Fiscalía como de la Policía Judicial, esto en razón de la falta por un lado de la infraestructura necesaria, como centros de vigilancia computarizada, las modernas herramientas de software y todos los demás implementos tecnológicos necesarios para la persecución de los llamados Delitos Informáticos, de igual manera falta la suficiente formación tanto de los Fiscales que dirigirán la investigación como del cuerpo policial que lo auxiliara en dicha tarea, dado que no existe hasta ahora en nuestra policía una Unidad Especializada, como existe en otros países como en Estados Unidos donde el FBI cuenta con el ComputerCrimeUnit, o en España la Guardia Civil cuenta con un departamento especializado en esta clase de infracciones. De otro lado también por parte de la Función Judicial falta la suficiente preparación por parte de Jueces y Magistrados en tratándose de estos temas, ya que en algunas ocasiones por no decirlo en la mayoría de los casos los llamados a impartir justicia se ven confundidos con la especial particularidad de estos delitos y los confunden con delitos tradicionales que por su estructura típica son incapaces de
Subsumir a estas nuevas conductas delictivas que tiene a la informática como su medio o fin. Por tanto es esencial que se formen unidades Investigativas tanto policiales como de la Fiscalía especializadas en abordar cuestiones de la delincuencia informática trasnacional y también a nivel nacional.

De otro lado en los últimos tiempos la masificación de virus informáticos globales, la difusión de la pornografía infantil e incluso actividades terroristas son algunos ejemplos de los nuevos delitos informáticos y sin fronteras que presentan una realidad difícil de controlar.

Con el avance de la tecnología digital en los últimos años, ha surgido una nueva generación de delincuentes que expone a los gobiernos, las empresas y los individuos a estos peligros (23).

2.2. INTRODUCCIÓN A BASES DE DATOS RELACIONALES

2.2.1. Lenguaje Estructurado de Consultas (SQL)

SQL (Structured Query Language) es un leguaje informático diseñado para la gestión de datos en sistemas de gestión de bases de datos relacionales RDBMS, y originalmente basado en álgebra relacional. Su ámbito de aplicación incluye datos de la consulta y actualización, la creación de esquemas y la modificación, y los datos de control de acceso (26).

Elementos del lenguaje

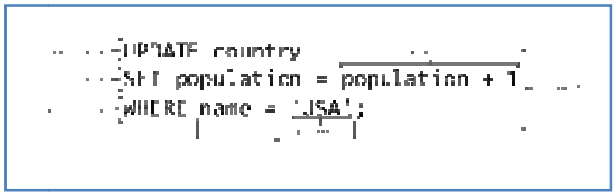


Figura II.2. Elementos del Lenguaje SQL

El lenguaje SQL se divide en varios elementos, incluyendo:

Cláusulas que son en algunos casos opcionales, elementos constitutivos de las declaraciones y consultas.

Expresión es que pueden producir cualquiera de los valores escalares o tablas consta de columnas y filas de datos.

Predicados que especifican las condiciones que pueden ser evaluados a SQL lógica de tres valores (3VL) los valores booleanos y de verdad que se utilizan para limitar los efectos de las declaraciones y preguntas, o para cambiar el flujo del programa.

Las consultas que recuperar los datos basados en criterios específicos.

Las declaraciones que pueden tener un efecto persistente en los esquemas y datos, o que puedan controlar las transacciones, el flujo del programa, las conexiones, sesiones, o de diagnóstico.
SQL también incluye la terminación de (";") coma declaración. Aunque no es necesario en cualquier plataforma, que se define como una parte estándar de la gramática de SQL.
Espacios en blanco insignificantes es generalmente ignorado en las sentencias SQL y consultas, lo que facilita al formato de código SQL para mejorar la legibilidad.

2.2.2. Almacenamiento de Datos

Un almacén de datos es una colección de datos orientada a un determinado ámbito, integrado, no volátil y variable en el tiempo, que ayuda a la toma de decisiones en la entidad en la que se utiliza. Se trata, sobre todo, de un expediente completo de una organización, más allá de la información transaccional y operacional, almacenado en una base de datos diseñada para favorecer el análisis y la divulgación eficiente de datos (especialmente OLAP, procesamiento analítico en línea). Los almacenes de datos contienen a menudo grandes cantidades de información que se subdividen a veces en unidades lógicas más pequeñas dependiendo del subsistema de la entidad del que procedan o para el que sea necesario.

Almacenamiento de datos con SQL Server

El motor de almacenamiento representa el corazón de un servidor SQL Server.
(OLTP), sistemas de datos tendrá que ser recuperado, añadidos o modificados en el motor de base de datos
La construcción de una instalación de almacenamiento capaz de escalar de acuerdo con estos requisitos es un trabajo duro. Expectativas de los usuarios han crecido fuera de todo reconocimiento en los últimos años

Técnicas de almacenamiento y recuperación de bases de datos

Las técnicas empleadas para almacenar bases de datos son sumamente importantes para la velocidad de acceso y recuperación de datos. Las técnicas dependen del tipo de

almacenamiento, el uso que se le da o se le dará a la base de datos, la estructura de la misma, el SGBD empleado, etc.
Las técnicas de almacenamiento son independientes de la base de datos, pero, de todas maneras, las mejores técnicas muchas veces pueden determinarse viendo la estructura de la base de datos, entre otras características.
Los encargados de elegir estas técnicas son los diseñadores y administradores de bases de datos, y dependen también de las capacidades del SGBD. En general, el SGBD ofrece diferentes opciones y técnicas para organizar los datos.

La idea es que los encargados de la base de datos encuentren las técnicas idóneas, o sea, aquellas que permitan la mayor velocidad posible de acceso a los datos. Una mala decisión en esta área puede resultar en una menor velocidad de acceso a la base de datos, o en un uso excesivo del espacio de almacenamiento, o incluso, puede aumentar la velocidad de consulta de una base de datos, pero disminuir la velocidad de actualización de la misma.

2.2.3. Permisos y Autenticación

Autenticación de SQL Server

La autenticación de SQL Server se basa en la lista de usuarios interno mantenido por el equipo de SQL Server. Esta lista no incluye a los usuarios de Windows NT, y es específica para el equipo de SQL Server. Los usuarios se crean y configuran mediante el SQL Server Enterprise Manager. Para utilizar este método de autenticación, realice los siguientes pasos:

- Si se conecta a través de Open DatabaseConnectivity (ODBC), en el Administrador de ODBC, elija la autenticación de SQL Server al configurar el origen de datos.
- En el ActiveX Data Objects (ADO) de cadena de conexión, son los parámetros "uid" y "personas con discapacidad" cuando utiliza ODBC, y "User ID" y "Contraseña" cuando utiliza el proveedor SQLOLEDB.
- Tanto la autenticación de SQL Server (seguridad estándar) y la autenticación de Windows NT (seguridad integrada) son los métodos de autenticación de SQL

Server que se utiliza para acceder a una base de datos SQL Server desde páginas Active Server (ASP).

Microsoft SQL Server ofrece a los administradores de dos opciones de realizar la autenticación de usuario: el modo de autenticación de Windows y el modo de autenticación mixta. Hacer la elección correcta afecta tanto a la seguridad y el mantenimiento de bases de datos de su organización.

Autenticación básica

La autenticación es el proceso de confirmación de la identidad de un usuario o equipo. El proceso normalmente consta de cuatro pasos:

1. El usuario hace una afirmación de la identidad, por lo general, proporcionando un nombre de usuario. Por ejemplo, yo podría hacer esta afirmación contando una base de datos que mi nombre de usuario es "mchapple".
2. El sistema pregunta al usuario a probar su identidad. El problema más común es una solicitud de una contraseña.
3. El usuario responde al desafío de proporcionar la prueba solicitada. En este ejemplo, me gustaría ofrecer la base de datos con mi contraseña
4. El sistema verifica que el usuario ha proporcionado una prueba aceptable, por ejemplo, comprobar la contraseña contra una base de datos local de contraseñas o utilizando un servidor de autenticación centralizado

Modos de autenticación de SQL Server

SQL Server 2005 ofrece dos opciones de modo de autenticación:

- **El modo de autenticación de Windows** requiere que los usuarios de Windows un nombre de usuario y contraseña válidos para acceder al servidor de base de datos. En los entornos empresariales, estas credenciales son normalmente las credenciales de dominio de Active Directory.
- **El modo de autenticación mixta** permite el uso de credenciales de Windows sino que los completa con locales de cuentas de usuario de SQL Server que el administrador puede crear y mantener dentro de SQL Server.

Selección de un modo de autenticación

La recomendación de las mejores prácticas de Microsoft es que se utiliza el modo de autenticación de Windows siempre que sea posible. El beneficio principal es que el uso de este modo le permite centralizar la administración de la cuenta para toda su empresa en un solo lugar: Active Directory. Esto reduce drásticamente las posibilidades de error o descuido.

Por ejemplo, considere el escenario donde un administrador de base de datos de confianza abandone su organización en términos poco amistosos. Si utiliza el modo de autenticación de Windows, la revocación de su acceso de los usuarios se lleva a cabo automáticamente cuando se deshabilite o elimine la cuenta del DBA de Active Directory. Si utiliza el modo de autenticación mixta, no sólo es necesario deshabilitar la cuenta del DBA de Windows, pero también tiene que peine a través de las listas de usuarios locales en cada servidor de base de datos para asegurar que no existen cuentas locales en el DBA puede saber la contraseña.

Autenticación de MySQL

MySQL 5.1 utiliza un protocolo de autenticación basado en un algoritmo de hash de la clave que es incompatible con la utilizada por los mayores (pre-4.1) clientes. Si usted actualiza su servidor a 4.0, intenta conectarse a él desde un cliente más viejo pueden fallar con el siguiente mensaje:

```
shell>mysql
Cliente no soporta el protocolo de autenticación solicitado por el
servidor; considerar la actualización de cliente de MySQL
```

Para resolver este problema, debe utilizar uno de los siguientes métodos:

- Actualizar todos los programas cliente para utilizar 4.1.1 o posterior biblioteca cliente.
- Cuando se conecta al servidor con un pre-4.1 del programa cliente, utilice una cuenta que todavía tiene un pre-4.1-clave al estilo.
- Restablecer la contraseña para pre-4.1 de estilo para cada usuario que necesite utilizar un pre-4.1 del programa cliente.
- Esto puede hacerse utilizando la instrucción SET PASSWORD y la OLD_PASSWORD() Función:

- mysql>**SET PASSWORD FOR**
- **' *some_user* '@' *some_host* ' = OLD_PASSWORD(' *newpwd* '); ->' *some_user* '@' *some_host* ' = OLD_PASSWORD(' *newpwd* ');**

Otra opción es utilizar **UPDATE** y **FLUSH PRIVILEGES**

mysql>**UPDATE mysql.user SET Password = OLD_PASSWORD(' *newpwd* ')**
->**WHERE Host = ' *some_host* ' AND User = ' *some_user* ';**
mysql>**FLUSH PRIVILEGES;**

Sustituya la clave que desea utilizar para *newpwd* en los ejemplos anteriores. MySQL no puede decir cuál es la clave original, así que tendrás que elegir uno nuevo.

- Indique al servidor que utiliza el algoritmo de hashing de claves antiguo:
  a) Inicie mysqld con --old-passwords opción --old-passwords
  b) Asigne una clave con formato antiguo a cada cuenta que tenga su clave actualizada al formato más largo 4,1. Puede identificar estas cuentas con la siguiente consulta:
     a. mysql>**SELECT Host, User, Password FROM mysql.user**
     b. ->**WHERE LENGTH(Password) > 16;**

Para cada registro de cuenta que aparece por la consulta, utiliza el Host y los valores de Usuario y asignarle una contraseña a través del OLD_PASSWORD() y, o bien la función SET PASSWORD o UPDATE tal como se describe anteriormente.

¿Qué es Autenticación?

Es básicamente el proceso de determinar que alguien es realmente quien dice ser.

Figura II.3. Autenticación

En SQL Server nos encontramos con tres niveles o capas en los cuales podemos gestionar la seguridad. El primero de ellos se encuentra a nivel de servidor, en él podemos gestionar quién tiene acceso al servidor y quién no, y además gestionamos que roles va a desempeñar. Para que alguien pueda acceder al servidor debe tener un inicio de sesión (login) asignado, y a éste se asignaremos los roles o funciones que puede realizar sobre el servidor.

El que alguien tenga acceso al servidor no quiere decir que pueda acceder a las bases de datos que se encuentran en él. Para ello hay que tener acceso a la siguiente barrera de seguridad, que es a nivel de base de dato. Para que un login tenga acceso a una base de datos, tenemos que crear en ella un usuario (user). Deberemos crear un usuario en cada una de las bases de datos a las que queramos que acceda un login.

Análogamente, el que un usuario tenga acceso a una base de datos no quiere decir que tenga acceso a todo su contenido, ni a cada uno de los objetos que la componen. Para que esto ocurra tendremos que irle concediendo o denegando permisos sobre cada uno de los objetos que la componen (8).

A continuación se puede observar un gráfico que refleja este modelo.

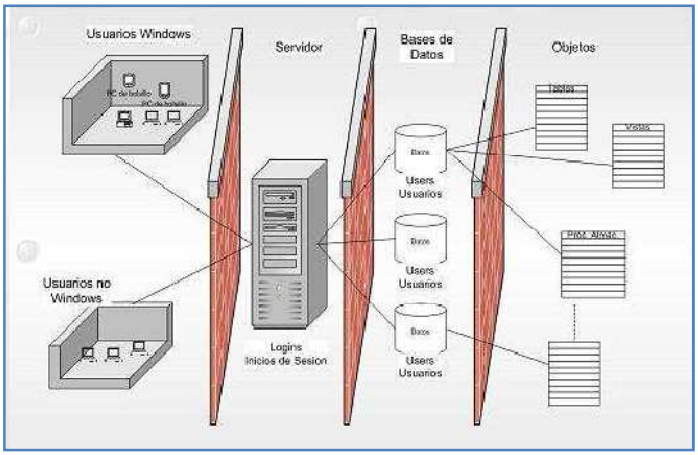


Figura II.4. Modelo de Autenticación

Mecanismos de Autenticación de SQL Server

MDAC: El cliente utilizará una DLL asociada con Microsoft Data Access Client (MDAC)

Socket connection: MDAC intentara establecer una conexión a una socket connection a SQL Server (22).

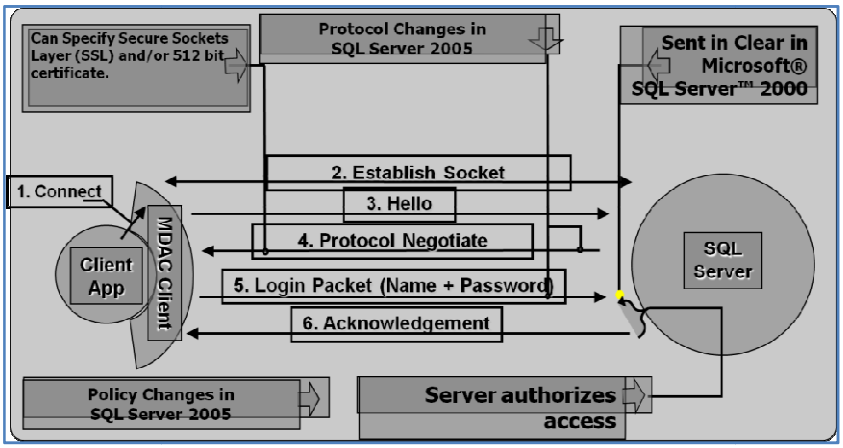


Figura II.5. Diagrama de Autenticación de SQL Server

Permisos

Los administradores de base de datos deberían analizar periódicamente los permisos de SQL Server para asegurarse de que no hay inicios de sesión y usuarios no deseados y el acceso de base de datos, respectivamente.

Al crear objetos de base de datos, se deben conceder permisos de forma explícita para que los usuarios tengan acceso a ellos. Cada objeto susceptible de protegerse tiene permisos que se pueden otorgar a una entidad de seguridad mediante instrucciones de permiso.

Esquema de permisos generales

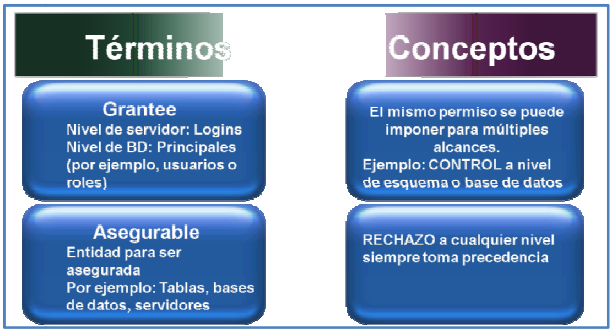


Figura II.6. Esquema de Permisos Generales

Permisos basados en funciones

Otorgar permisos a funciones en lugar de a usuarios simplifica la administración de la seguridad. Los conjuntos de permisos asignados a funciones los heredan todos los miembros de la función. Es más fácil agregar o quitar usuarios de una función que

volver a crear conjuntos de permisos distintos para cada usuario. Las funciones se pueden anidar. Sin embargo, la existencia de demasiados niveles de anidamiento puede reducir el rendimiento. También se puede agregar usuarios a funciones fijas de bases de datos para simplificar los permisos de asignación.

A partir de SQL Server 2005, se pueden conceder permisos a nivel de esquema. Los usuarios heredan automáticamente los permisos en todos los objetos nuevos creados en el esquema; no es necesario otorgar permisos cuando se crean objetos nuevos (9).

Permisos mediante código basado en procedimiento

El encapsulamiento del acceso a los datos a través de módulos tales como procedimientos almacenados y funciones definidas por el usuario brinda un nivel de protección adicional a la aplicación. Se puede evitar que los usuarios interactúen directamente con objetos de la base de datos otorgando permisos sólo a procedimientos almacenados o funciones, y denegando permisos a objetos subyacentes tales como tablas. SQL Server lo consigue mediante encadenamiento de propiedad (4).

Tabla II.II Instrucciones de Permiso

INSTRUCCIÓN DE PERMISO	DESCRIPCIÓN
GRANT	Concede un permiso.
REVOKE	Revoca un permiso.
DENY	DENY revoca un permiso de manera que no pueda ser heredado. DENY tiene prioridad sobre todos los permisos.

Fuente: http://msdn.microsoft.com/es-es/library/bb669084.aspx

Elaborador por: Microsoft Corporation

Encriptación en SQL Server

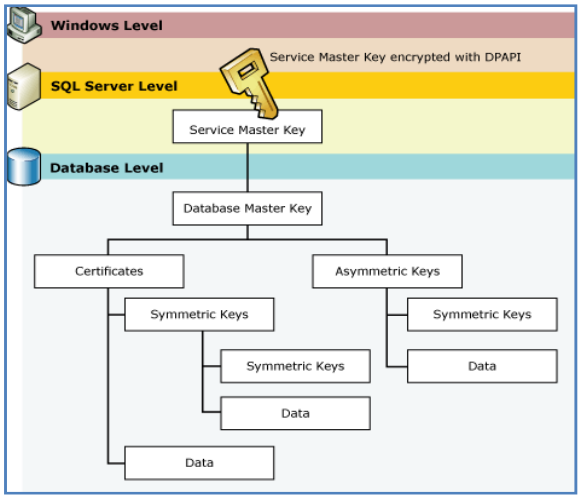


Figura II.7. Jerarquía de encriptación

Con SQL Server 2005 viene un sistema de encripción jerárquico basado en una clave maestra de servicio (Service Master Key), esta clave es generada automáticamente cuando se instala SQL Server 2005. El motor de base de datos utiliza la clave maestra de servicio para encriptar los siguientes objetos.

- Passwords de Servidores Vinculados (Linked Server Passwords)
- Cadenas de Conexión (Connection Strings)
- Credenciales de Cuentas (Account Credentials)
- Todas las Claves maestras de la base de datos

A la clave maestra de servicio se le debe sacar un backup y almacenarla en un sitio seguro y fuera de línea. Esto para poder administrar más fácilmente ya sea hacer bakcups o restaurar la clave maestra de servicio en caso de que sea necesario.

El siguiente nivel en la jerarquía de encripcion es el nivel de base de datos acá se crea la clave maestra de base de datos (Database master key), esta clave es opcional y es utilizada para encriptar certificados y claves en la base de datos.

SQL Server almacena una copia de la clave maestra de base de datos en la base de datos master y a su vez es encriptada con la clave maestra de servicio. Otra copia es almacenada en la base de datos encriptada con un password (2).

SQL Server 2005 cifra los datos con una infraestructura de cifrado jerárquico y administración de claves. Cada capa cifra la capa inferior utilizando una combinación de certificados, claves asimétricas y claves simétricas.

2.3. SEGURIDAD EN BASE DE DATOS

Las bases de datos son componentes claves de cualquier aplicación basada en web, permitiendo que los sitios web provean contenido dinámico. Debido a que información considerablemente sensible o secreta puede ser almacenada en una base de datos, usted debe considerar seriamente la protección de sus bases de datos.

Para recuperar o almacenar cualquier información necesita conectarse a la base de datos, enviar una consulta válida, recoger el resultado y cerrar la conexión. El lenguaje de consultas usado comúnmente en estas interacciones es el Lenguaje de Consultas Estructurado (SQL por sus siglas en inglés).

Los datos pueden almacenarse bajo diferentes tecnologías, radicalmente diferentes entre sí. Desde las ya venerables bases de datos jerárquicas, bases de datos orientadas a objetos o nativas XML(usando lenguajes de consulta particulares, como OQL o XQuery), sin embargo en la actualidad el modelo relacional es quien reina por doquier, salvo en algunas aplicaciones particulares.

Se puede señalar que las bases de datos relacionales posee varios defectos en cuanto seguridad se refiere, aun cuando los sistemas de base de datos comerciales son increíbles y enormemente complejas en la actualidad, pensemos por ejemplo en Oracle 10g. Todo sistema complejo tiene defectos, los defectos derivan en vulnerabilidades, y a través de estas vienen los ataques y el uso indebido.

Tabla II.III Vulnerabilidades de bases de datos relacionales ampliamente difundidas

DBMS	VULNERABILIDADES CONOCIDAS
Oracle 10g – 23	(22 de severidad alta)
Microsoft SQL Server 2000 – 39	(21 de severidad alta)
IBM DB2 UDB 7.x y 8.x – 5	(3 de severidad alta)
MySQL 5.x – 17	(3 de severidad alta)

Fuente: http://www.als-es.com/home.php?location=recursos/articulos/seguridad-en-bases-de-datos

La seguridad de los datos depende de muchos factores. Observamos en la siguiente figura los puntos tradicionales de 'fricción' en materia de seguridad en el ámbito de las bases de datos relacionales, con ejemplos de las bases de datos mencionadas (25).

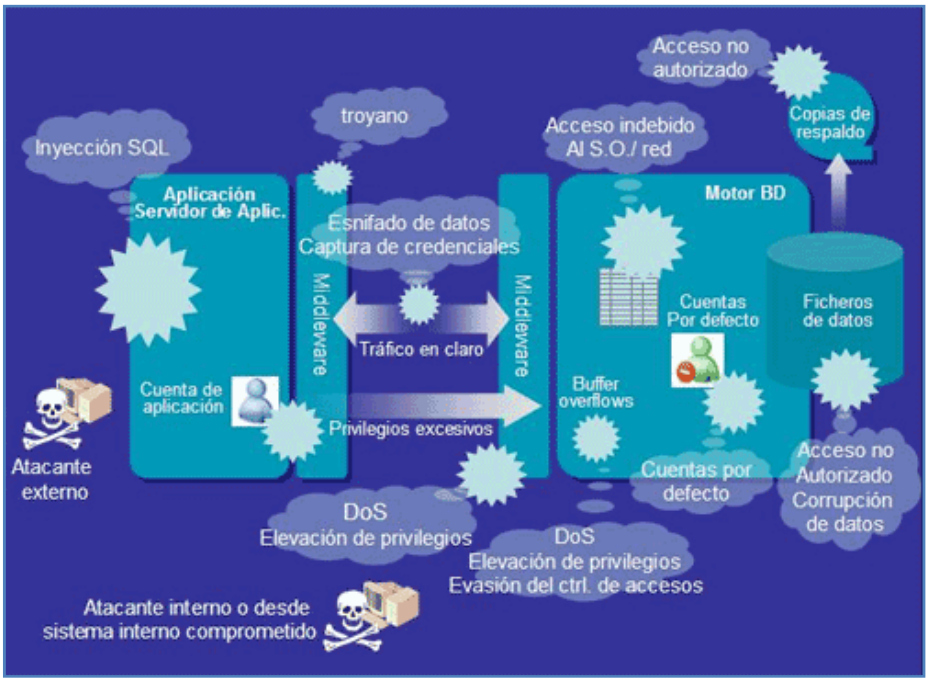


Figura II.8. Puntos de 'fricción' de las bases de datos relacionales

2.3.1. Tipos de Seguridad

En la actualidad se acostumbra hablar de dos tipos de mecanismos de seguridad en las bases de datos (18):

- **Los mecanismos de seguridad discrecionales** se usan para otorgar privilegios a los usuarios, incluida la capacidad de tener acceso a archivos, registros o campos de datos específicos en un determinado modo.
- **Los mecanismos de seguridad obligatorios** sirven para imponer igualdad de múltiples niveles clasificando los datos y los usuarios en varias clases (o niveles) de seguridad e implementando después la política de seguridad apropiada de la organización.

Un problema de seguridad común a todos los sistemas de computo es el de evitar que personas no autorizadas tengan acceso al sistema, ya sea para obtener información o para efectuar cambios mal intencionados en una porción de la base de datos. El mecanismo de seguridad de un SGBD debe incluir formas de restringir el acceso al sistema como un todo. Esta función se denomina **control de acceso** y se pone en prácticas creando cuentas de usuarios y contraseñas para que el SGBD controle el proceso de entrada al sistema.

Otra técnica de seguridad es el cifrado de datos, que sirven para proteger datos confidenciales que se transmiten por satélite o por algún otro tipo de red de comunicaciones. El cifrado puede proveer protección adicional a secciones confidenciales de una base de datos.
Los datos se codifican mediante algún algoritmo de codificación. Un usuario no autorizado que tenga acceso a los datos codificados tendrá problemas para descifrarlos, pero un usuario autorizado contara con algoritmos (o claves) de codificación o descifrado para descifrarlos.

2.3.2. Tipos de Ataque

Hoy en día las Bases de Datos son accesibles al público desde Internet y compartidas con proveedores, clientes y socios, ya que estas son más útiles cuando su información está disponible a más personas. Sin embargo esto aumenta la amenaza a su seguridad, por lo cual se necesita proteger todos los niveles

La mayoría de las empresas tiene alguna aplicación web disponible para Internet y/o para uso interno, comúnmente obtienen información de un servidor de base de datos.

Estas bases de datos parecen estar seguras debido a que los usuarios no están directamente conectados a ellas, sino a través del servidor web, pero en realidad estas son frecuentemente blanco de ataques a través de la red de datos o vía web.

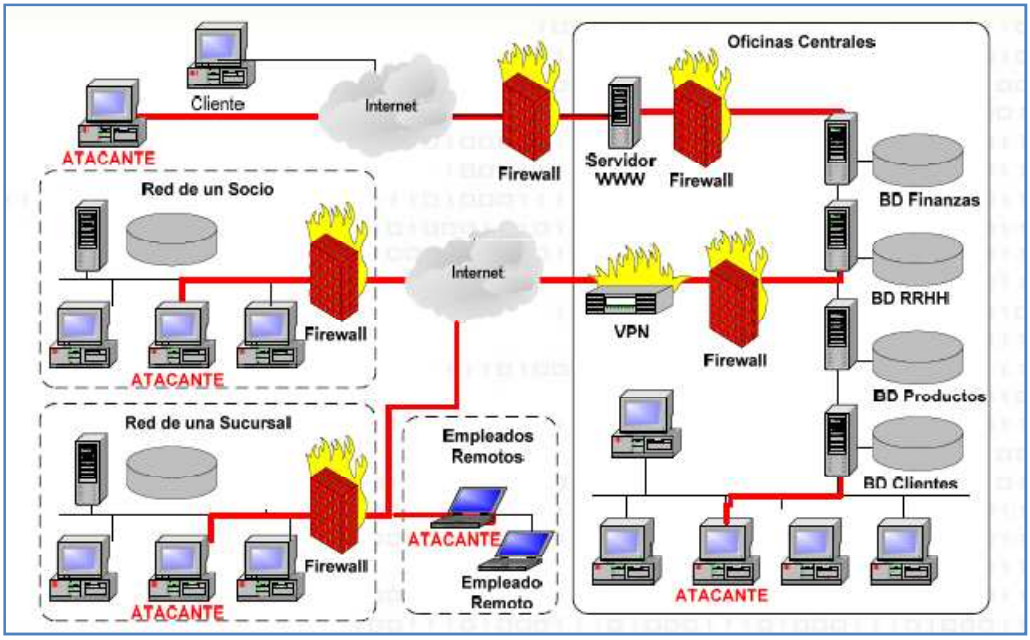


Figura II.9. Escenario de Ataques a Bases de Datos

Si bien entre los profesionales que conformamos la comunidad de seguridad informática, eventualmente puede surgir alguna divergencia al momento de definir los diferentes tipos de ataques en general, en aquellos relacionados con Bases de Datos el tema es bastante más sencillo, o dicho de otro modo, la definición del tipo de ataque se encuentra bastante estandarizada.

En líneas generales, podemos decir que los ataques a base de datos suelen formar parte de uno de los siguientes dos grandes grupos: *Ataques que No Requieren Autenticación* y *Ataques que Requieren Autenticación*.

Los ataques que *No Requieren Autenticación*, son los que generalmente suelen tener mas prensa, puesto que no se requiere presentar "credenciales validas" antes de lanzar el ataque. Dentro de esta categoría, se encuentran por ejemplo, algunas de las explotaciones de Buffer Overflow.

Otros ataques dignos de ser mencionados, dentro de aquellos que *No Requieren Autenticación*, son aquellos por medio de los cuales se intenta obtener un nombre de usuario y contraseña validos en el sistema objetivo mediante técnicas tales como la adivinación y los ataques de fuerza bruta o diccionario.
Por su parte, los *Ataques que Requieren Autenticación* deben ser lanzados por los poseedores de credenciales. Este hecho se encuentra directamente relacionado con la gran cantidad de vulnerabilidades existentes dentro de esta categoría, puesto que en este escenario, el usuario posee acceso al sistema a objetivo y cuenta con muchas más oportunidades al momento de lanzar un ataque, en parte fruto de la funcionalidad propia de la aplicación para la cual se obtiene un juego de credenciales válidas.

2.3.2.1. Ataques de Fuerza Bruta o Diccionario

La fuerza bruta describe un estilo de programación primitiva, en la que el programador se basa en la potencia de procesamiento de la computadora en lugar de utilizar su inteligencia para simplificar el problema, a menudo haciendo caso omiso de los problemas de escala y la aplicación de métodos adecuados a las pequeñas ingenuo problemas directamente a las grandes. El término también puede ser usado en referencia al estilo de programación: los programas de fuerza bruta se escriben de una manera heavy handed, tedioso, lleno de repeticiones y carece de elegancia o la abstracción.
Cualquier intento criminal para acceder a un sistema informático por la ejecución repetida de una acción. Un ejemplo de esto es un intento de descifrar

un mensaje que ha sido objeto ENCRYPTION varias veces tratando a un gran número de claves para DECRYPTION. Si el método de cifrado es seguro un ataque con éxito utilizando la fuerza bruta tendría que emplear una cantidad excesivamente grande de potencia de los ordenadores. Los ataques de fuerza bruta sobre los regímenes tales como el Data Encryption Standard y el protocolo Secure Sockets Layer han tenido éxito. A menudo han llevado a cabo con el apoyo activo de los desarrolladores de los sistemas, sin embargo, los recursos necesarios y el tiempo necesario para que el ataque haya sido tan prohibitivo que los sistemas son considerados como seguros. El término también puede ser utilizado para describir los ataques a una red informática que se basan en BARRIDO ATAQUES.

2.3.2.2. Inyección SQL

Inyección SQL un tipo de ataque a una base de datos en el nivel de la validación de las entradas a la base de datos de una aplicación. El origen es el filtrado incorrecto de las variables utilizadas en las partes del programa con código SQL. Es, de hecho, un error de una clase más general de vulnerabilidades que puede ocurrir en cualquier lenguaje de programación o de script que esté incrustado dentro de otro.

Una inyección SQL sucede cuando se inserta o "inyecta" un código SQL "invasor" dentro de otro código SQL para alterar su funcionamiento normal, y hacer que se ejecute maliciosamente el código "invasor" en la base de datos.

La inyección SQL es un problema de seguridad informática que debe ser tomado en cuenta por el programador para prevenirlo. Un programa hecho con descuido, displicencia, o con ignorancia sobre el problema, podrá ser vulnerable y la seguridad del sistema puede quedar ciertamente comprometida. Esto puede suceder tanto en programas ejecutándose en computadores de escritorio, como en páginas Web, ya que éstas pueden funcionar mediante programas ejecutándose en el servidor que las aloja (20).

Una inyección SQL sucede cuando se inserta o "inyecta" un código SQL "invasor" dentro de otro código SQL para alterar su funcionamiento normal, y hacer que se ejecute maliciosamente el código "invasor" en la base de datos.
La inyección SQL es un problema de seguridad informática que debe ser tomado en cuenta por el programador para prevenirlo. Un programa hecho con descuido, displicencia, o con ignorancia sobre el problema, podrá ser vulnerable y la seguridad del sistema puede quedar ciertamente comprometida. Esto puede suceder tanto en programas ejecutándose en computadores de escritorio, como en páginas Web, ya que éstas pueden funcionar mediante programas ejecutándose en el servidor que las aloja.

Ataque blind SQL Injection.

Se considera un ataque a ciegas, es decir, sin conocer nada sobre el server (Versión de SQL, nombre de las tablas, numero de tablas, etc., que deberemos saber para concluir el ataque y para saber defendernos.)
Consiste en obtener el número de columnas de la BD, bien para sacar el numero de columnas de la base de datas (BD,DB), vamos a inyectar un código que cause un conflicto al llegar a un numero de columna, el cual no se encuentra en la base de datos, para esto vamos a utilizar la clausulaorderby. Este tipo de ataque se basa en ordenar columnas hasta llegar a la última. Así al poner la siguiente, al no existir, nos devolverá un error tipo:

Unknown column ‘numerodecolumna’ in ‘order clause’

El error puede sufrir variaciones pero lo que nos interesa es que nos devuelva el unknowncolumn y el número que es lo que nos indica que columna es la que no está definida.

Inyección SQL en MySQL

En 'magic_quotes_gpc', se encuentra el "GPC" para GET / POST / COOKIE. Esta configuración está habilitada por defecto en las versiones más recientes, por lo que si el valor de ser presentados por el usuario se está coloca en una variable de cadena:

*$query = "SELECT * FROM user where user = '". $_REQUEST ('user'(. """;*

La inyección de SQL es imposible. Sin embargo, si el valor está siendo colocado en un no delimitado parte de la consulta, como un valor numérico, tabla o columna de nombre:

$query = "SELECT * FROM user order by " . $_REQUEST ('user'(;

o

$query = "SELECT * FROM user where max_connections = " .$_REQUEST('user'(;

Entonces inyección de SQL es todavía posible. Una forma posible de tratar con el teclado numérico problema en PHP / MySQL es delimitar * all * los datos del usuario entre comillas simples, incluyendo números. La comparación seguirá funcionando, pero magic_quotes_gpcprotegerá frente a los atacantes escapar de la cadena.

Obviamente, si "magicquotes" está desactivada, la inyección de SQL es siempre posible, dependiendo de sobre la forma en la entrada del usuario se valida. Suponiendo que el atacante es capaz de montar un ataque de inyección SQL, la pregunta es, entonces, ¿Qué pueden hacer? Una lista de las zonas de mayor peligro se ofrece a continuación (15):

- UNION SELECT
- LOAD_FILE function
- LOAD DATA INFILE statement
- SELECT ... INTO OUTFILE statement
- BENCHMARK function

2.3.2.3. Buffer Overflow

El desbordamiento de búfer es probablemente la forma más conocida de la vulnerabilidad de software en cuanto a seguridad. La mayoría de los desarrolladores de software saben lo que es una vulnerabilidad de desbordamiento de búfer, pero los ataques de desbordamiento de búfer siempre en contra de lo legal y aplicaciones recién desarrolladas son todavía muy comunes. Parte del problema se debe a la gran variedad de formas de

desbordamientos de búfer, y en parte es debido al error de técnicas expuestas para prevenirlos.

Los desbordamientos de búfer no son fáciles de descubrir y aún cuando se descubre uno, es generalmente muy difícil de explotar. Sin embargo, los atacantes han conseguido identificar a los desbordamientos de búfer en una asombrosa gama de productos y componentes.

Funcionamiento básico

El principio operativo de un desbordamiento de búfer guarda una relación muy estrecha con la arquitectura del procesador en la que se ejecuta una aplicación vulnerable.

Los datos ingresados en una aplicación se almacenan en la memoria de acceso aleatorio en una zona que se conoce como búfer. Un programa con un diseño correcto debería estipular un tamaño máximo para los datos de entrada y garantizar que no superen ese valor.

Las instrucciones y los datos de un programa en ejecución se almacenan temporalmente en forma adyacente en la memoria, en una zona llamada pila. Los datos ubicados después del búfer contienen una dirección de retorno (que se denomina puntero de instrucción) que le permite al programa continuar su tiempo de ejecución. Si el tamaño de los datos es mayor que el del búfer, la dirección de retorno se sobrescribe y el programa leerá una dirección de memoria no válida generando una violación de segmento en la aplicación.

Un pirata informático con un sólido conocimiento técnico puede asegurarse de que la dirección de memoria sobrescrita corresponda a una real, por ejemplo, una que esté ubicada en el mismo búfer. Como tal, al ingresar las instrucciones en el búfer (el código arbitrario), es fácil para él ejecutar este procedimiento.

Por lo tanto, es posible incluir instrucciones en el búfer que permitan abrir un intérprete de comandos (shell) permitiendo que el pirata tome control del sistema. Este código arbitrario que posibilita la ejecución del intérprete de comandos se conoce como código de shell o shellcode.

Descripción técnica

Un desbordamiento de búffer ocurre cuando los datos que se escriben en un búffer corrompen aquellos datos en direcciones de memoria adyacentes a los destinados para el búffer, debido a una falta de validación de los datos de entrada. Esto se da comúnmente al copiar cadenas de caracteres de un búffer a otro.

Desbordamiento de búfer y Aplicaciones Web

Los agresores utilizan los desbordamientos de búfer a la ejecución de corrupción de la pila de una aplicación web. Mediante el envío de insumos cuidadosamente diseñada para una aplicación Web, un atacante puede provocar que la aplicación web ejecute código arbitrario.

Los fallos de desbordamiento de búfer puede estar presente tanto en el servidor web o aplicaciones que sirven a los aspectos estáticos y dinámicos del sitio, o la aplicación web en sí. Los desbordamientos de búfer en los productos de servidor utilizado es probable que sean ampliamente conocidos y pueden suponer un riesgo significativo para los usuarios de estos productos.

Errores de desbordamiento de búfer en las aplicaciones web personalizadas tienen menos probabilidades de ser detectados porque no será normalmente un número mucho menor de los hackers tratando de encontrar y explotar tales fallas en una aplicación específica. Si se descubre en una aplicación personalizada, la capacidad de explotar el fallo (aparte de choque de la demanda) se reduce significativamente por el hecho de que el código fuente y mensajes de error de aplicación general no están a disposición de los piratas informáticos (6).

Entornos afectados

Casi todos los servidores web conocidos, servidores de aplicaciones y entornos de aplicaciones Web son vulnerables a desbordamientos de búfer, la excepción notable son los entornos escritos en lenguajes interpretados como Java o Python, que son inmunes a estos ataques (a excepción de los desbordamientos de su mismo interpretor).

Lenguajes: C, C++, Fortran, Assembly

Plataformas de operación: Todos, aunque parcial, las medidas preventivas pueden ser utilizados, en función del entorno.

2.3.3. Errores Humanos

Se ha dicho que las computadoras son realmente perfectas. La razón detrás de esta afirmación es que si usted profundiza lo suficiente, detrás de cada error computacional encontrará el error humano que lo causó. En esta sección se exploran los tipos de errores humanos más comunes y sus impactos.

Errores humanos del usuario final

Los usuarios pueden cometer errores que podrían tener un impacto muy serio. Sin embargo, debido a que su ambiente normalmente no tiene muchos privilegios, los errores tienden a ser de naturaleza localizada. Puesto que la mayoría de los usuarios interactúan exclusivamente con una computadora por una o más aplicaciones, usualmente es dentro de las aplicaciones que ocurren la mayoría de los errores.

Uso inapropiado de las aplicaciones

Cuando las aplicaciones son usadas inapropiadamente, pueden ocurrir varios problemas:

- Archivos sobreescritos inadvertidamente
- Datos incorrectos utilizados como entrada a una aplicación
- Archivos no claramente nombrados u organizados
- Archivos borrados accidentalmente

La lista puede continuar, pero esto es suficiente para ilustrar la situación. Puesto que los usuarios no tienen privilegios de super usuario, los errores que cometen están usualmente limitados a sus propios archivos. Como tal, el mejor enfoque es dividido:

Errores del personal de operaciones

Los operadores tienen una relación más profunda con las computadoras de una organización que los usuarios finales. Mientras que los errores de un usuario tienden a ser orientados a aplicaciones, los de los operadores tienden a llevar a cabo un rango más amplio de tareas. Aunque la naturaleza de las tareas haya sido dictada por otros, algunas de estas tareas pueden incluir el uso de utilidades a nivel del sistema, donde el potencial para daños más amplios debido a errores es mayor. Por lo tanto, los tipos de errores que

un operador puede hacer se centran en la habilidad de un operador de seguir procedimientos que hayan sido desarrollados para su uso.

Errores del Administrador del Sistema

A diferencia de los operadores, los administradores de sistemas realizan una variedad de tareas usando las computadoras de la organización. También a diferencia de los operadores, las tareas que los administradores de sistemas llevan a cabo a menudo no están basadas en procedimientos documentados.

En consecuencia, los administradores de sistemas a veces crean trabajo adicional para sí mismos cuando no tienen cuidado en lo que están haciendo. Durante el curso de llevar a cabo las responsabilidades diarias, los administradores de sistemas tienen acceso más que suficiente a los sistemas computacionales (sin mencionar los privilegios de super usuario) como para afectar accidentalmente los sistemas.

Los administradores de sistemas cometen errores de configuración o durante el mantenimiento.

Errores de configuración

Los administradores de sistemas a menudo deben configurar varios aspectos de un sistema computacional. Esta configuración incluye:

- Correo electrónico
- Cuentas de usuarios
- Red
- Aplicaciones

La lista puede extenderse mucho más. La tarea actual de configurar varía en gran medida; algunas tareas requieren editar un archivo de texto (usando cualquiera de los cientos de sintaxis de archivos de configuración), mientras que otras tareas requieren la ejecución de alguna utilidad de configuración.

El hecho de que estas tareas son manejadas de forma diferente es simplemente un reto adicional al hecho básico de que cada tarea de configuración requiere un conocimiento diferente. Por ejemplo, el conocimiento requerido para configurar un agente de transporte de correo es fundamentalmente diferente al conocimiento requerido para configurar una conexión de red.

Dado todo esto, quizás debería ser una sorpresa que solamente se cometen unos pocos errores. En cualquier caso, la configuración es y seguirá siendo, un reto para los administradores de sistemas. ¿Hay algo que se pueda hacer para hacer el proceso menos susceptible a errores?

Errores cometidos durante el mantenimiento

Este tipo de errores pueden ser insidiosos porque se hace muy poca planificación o seguimiento durante el mantenimiento de día a día.

Los administradores de sistemas ven el resultado de estos errores diariamente, especialmente de los usuarios que juran que no cambiaron nada - simplemente la computadora se echó a perder. El usuario que afirma esto usualmente no se recuerda qué fue lo que hizo y cuando le pase lo mismo a usted, probablemente usted tampoco recuerde lo que hizo.

Errores de Servicio Técnico

Algunas veces la propia gente que se supone debería ayudarlo a mantener sus sistemas funcionando confiablemente, son los que complican más las cosas. Esto no se debe a ninguna conspiración; es simplemente por el hecho de que cualquiera que esté trabajando en una tecnología por alguna razón, arriesga el hacer esa tecnología inoperable. El mismo efecto es en el trabajo cuando los programadores reparan un fallo pero terminan creando otro.

CAPÍTULO III

MODELOS DE ANÁLISIS FORENSE

3.1. REVISIÓN DE MODELOS DE ANÁLISIS FORENSE

Una de las principales formas en las que los investigadores tratan de entender la base científica de una disciplina es la construcción de modelos que reflejen sus observaciones. El área de la Informática Forenses Digital es una ciencia en constante evolución, y que con el avance tecnológico esta ha cambiando de una de una simple destreza a una verdadera ciencia forense. Debido a las circunstancias previamente expuestas, es importante la revisión de los modelos de investigación más aceptados en esta disciplina en la actualidad, ya que permite entender de una mejor manera los procedimientos y estándares que rigen hoy la informática forense en el mundo.

Un buen modelo de investigación de informática forense debe contar con una serie de principios los cuales se exponen a continuación (21):

Principio 1: Considerar el sistema entero.
Principio 2: Guardar la información de registro a pesar de que el sistema falle en su totalidad.
Principio 3: Considerar los efectos de los eventos, no solo las acciones que los causan.

Principio 4: Considerar el contexto para ayudar a la interpretación y el entendimiento de significado de un evento.

Principio 5: Presentar los eventos de manera en que puedan ser analizados y entendidos por un analista forense.

Cualidades

Además de los principios anteriormente mencionados, un modelo de investigación para la informática forense debe tener una serie de cualidades adicionales las cuales se expondrán a continuación (21):

- La habilidad de guardar registro de todo.
- Disposición de métricas automatizadas, como la longitud de un path o ruta absoluta de un archivo, y un parámetro de ajuste que permita que un analista forense pueda decidir qué tipo de información es importante y que tipo no.
- La capacidad de analizar datos a múltiples niveles de extracción, incluyendo aquellos que no pertenecen explícitamente al sistema en cuestión.
- La capacidad de establecer límites y de reunir datos de los hasta ahora desconocidos ataques y métodos de ataque actuales.
- La habilidad de recolectar información sobre las condiciones de antes (causa) y después (efecto) de ocurrido el evento.
- La habilidad de modelar ataques multifacéticos.
- La capacidad de traducir entre los datos registrados y los acontecimientos actuales.

A continuación se expondrán una serie de modelos de investigación en el área de informática forense, con lo cual se podrá observar la evolución del área desde sus primeros días hasta la actualidad, además de proporcionar un mejor entendimiento de los procedimientos y estándares actuales de la informática forense en el mundo. Entre los modelos revisados que tienen mayor importancia están los siguientes: Modelo Digital Forensic Research Workshops(DFRW), Modelo Forense Digital Abstracto, Modelo Forense The Cyber Forensic Field Triage Process Model(CFFTPM) y el Modelo Básico Forense.

3.1.1. Modelo Digital Forensic Research Workshops (DFRW)

El uso común de la tecnología ha generado problemas sociales en donde se requiere de la intervención de las ciencias forense. De igual forma, estos problemas han sido de alto impacto social y económico, tanto que la última década se han desencadenado avances sustanciales que permiten solucionar problemas cuya causa son los delitos e incidentes informáticos. De acuerdo a lo establecido por el organismo conocido como Digital Forensic Reserch Workshop(DFRWS) creado en el 2001 en Nueva York.

Este modelo puede ser clasificado como un modelo de compresión ya que tiende a cubrir algunas de las etapas en las que no sean judiciales en algún modelo anterior, tales como la etapa de presentación.

El modelo de DFRW está dividido en siete fases:

1. Identificación
2. Preservación
3. Recolección
4. Inspección
5. Análisis
6. Presentación
7. Decisión

La mayoría de los pasos son secuenciales en la naturaleza, sin embargo, el proceso no debe ser inamovible. Si en la fase de análisis de una nueva fuente potencial de las pruebas se encuentra, entonces la preservación, la Colección, el examen y las fases de análisis se repite (1).

Identificación: Esta fase es precipitada ya sea por la delincuencia que se ha informado o de un incidente dentro de una organización.

Preservación: En esta fase se inicia con los procedimientos de gestión de casos, incluyendo la cadena de custodia. A continuación se debe duplicar y conservar la Evidencia.

Recolección: Los datos conservados se recogen, se usa software autorizado, los métodos y el hardware. Por ejemplo, en esta fase los archivos temporales de Internet se encuentran y se almacena para la fase de análisis.

Inspección: Las fuentes potenciales de las pruebas son examinadas mediante el filtrado y técnicas de coincidencia de patrón. La idea es reducir el volumen de las pruebas y determinar las correspondientes piezas de evidencia que se utilizarán para recrear la escena del crimen o el incidente.

Análisis: En la fase de análisis se recopilas y reúnen las pruebas para reconstruir la escena del crimen.

Presentación: En la fase de presentación, la investigación es bien documentada y presentada como un testimonio o como un informe a un superior en relación con un incidente.

Decisión: Por último, en la fase final se toma una decisión realizada en relación con un incidente, o un veredicto que se haga en un tribunal de justicia (1).

3.1.2. Modelo Forense Digital Abstracto

Este modelo llamado Modelo Forense Digital Abstracto, evoluciona del anterior y se basa en los siguientes procedimientos (26). El diagrama de la Figura 3.10muestra las fases que componen el manejo de un incidente en una investigación:

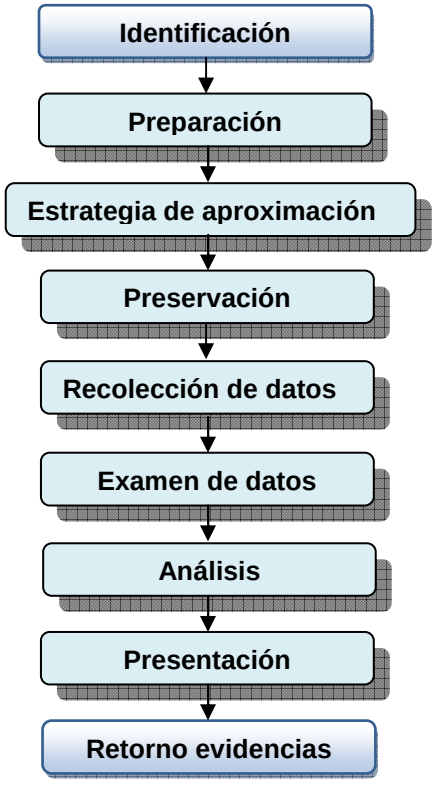


Figura III.10. Diagrama de Modelo Forense Digital Abstracto

Identificación: Consiste en el reconocimiento de un incidente y la determinación del tipo de incidente. Este paso no tiene que ver explícitamente con el campo forense pero si tiene un impacto significante en los demás pasos.

Preparación: Consiste en la preparación de las herramientas, técnicas, monitoreo, manejo y administración del personal de soporte.

Estrategia de aproximación: Consiste en diseñar un plan que permita maximizar la recolección de la evidencia minimizando el impacto a la víctima.

Preservación: Consiste en aislar, asegurar y preservar el estado de la evidencia física y digital. Esto incluye prevenir que cualquier persona utilice el sistema en cuestión ya que puede terminar en la alteración o pérdida de la evidencia digital.

Recolección de datos: Consiste en grabar la escena física tal cual como está y duplicar la evidencia digital recolectada usando procedimientos estandarizados y mundialmente reconocidos.

Examen de datos: Consiste en la búsqueda sistemática y profunda de evidencia digital que esté relacionada con el caso investigado. Es necesario realizar una documentación detallada sobre el trabajo realizado en esta fase del proceso.

Análisis: Consiste en analizar los resultados del examen de datos, usando métodos y técnicas adecuadas, que permitan obtener respuestas concretas y aceptables.

Presentación: Consiste en resumir y proveer una explicación de las conclusiones obtenidas. Este documento debe ser escrito por una persona experta en leyes que use la terminología correspondiente.

Retorno de evidencias: Consiste asegurar que la devolución de la evidencia física y digital sea devuelta a su dueño en perfectas condiciones.

3.1.3. Modelo Forense The Cyber Forensic Field Triage Process Model (CFFTPM)

El modelo puede llevarse a cabo en el escenario que ofrece el beneficio adicional de tener un circuito de retroalimentación con los investigadores, lo que permite al analista de computación forense modificar sus búsquedas basadas en las aportaciones de los investigadores principales y aquellos en contacto directo con el sospechoso. Debido a la

necesidad de información que se obtenga en un plazo relativamente corto, el modelo implica generalmente un sitio/campo de analisis del sistema informático en cuestión.

Los enfoques del modelo son los siguientes:

1. Encontrar evidencia utilizable inmediatamente
2. Identificar a las víctimas en situación de riesgo agudo
3. Guía de la investigación en curso
4. Identificar posibles roles, y
5. Evaluar con precisión el peligro del delincuente a la sociedad.

Mientras que al mismo tiempo proteger la integridad de las pruebas y/o las posibles pruebas para el examen y análisis.

El CFFTPM utiliza fases derivadas del Modelo de Procesos de Investigación Digital Integrada de Carrier y Spafford (2002) y el Análisis Digital de Escena del Cirmen (DCSA) modelo desarrollado por Rogers (2006). Las fases son: la planificación, triage, uso/perfiles de usuario, cronología / línea de tiempo, la actividad de Internet, y Caso específico (ver Figura 3.11). Estas seis fases constituyen un alto nivel de categorización y cada fase tiene varias sub-tareas y las consideraciones que varían de acuerdo a las particularidades del caso, el sistema de archivos y sistema operativo de investigación, etc El uso de categorías de orden superior permite que el proceso modelo para ser generalizados a través de diversos tipos de investigaciones que se ocupan de la evidencia digital.

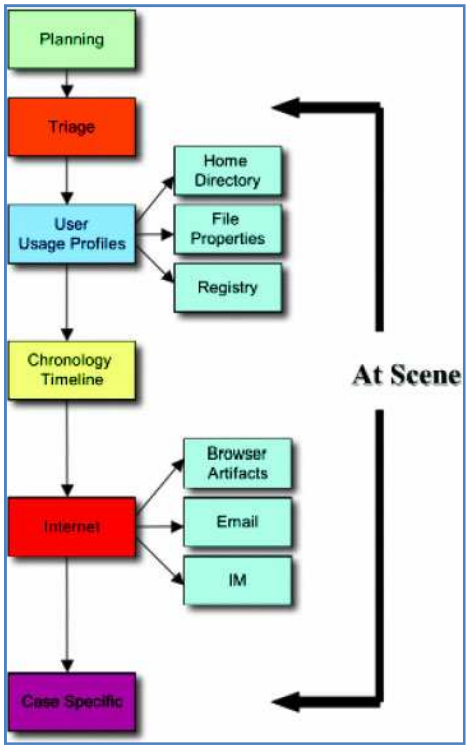


Figura III.11. Fases de CFFTPM

Planificación

La primera fase de la CFFTPM es la planificación adecuad. Idealmente, un investigador tendrá una matriz que cuantifica las diversas posibilidades de la escena del crimen, el sospechoso y la evidencia digital y califica la experiencia de los diferentes investigadores en el equipo de investigación. Para el investigador principal, esta matriz se utiliza para definir lo que se conoce y lo que no sabe lo que ayuda a determinar lo que se quiere ser conocido.

La fuerza inicial determina el número de sospechosos, y cualquier otras cohortes que se trate, pero también podrían incluir conocidos o posibles capacidades del sospechoso. La actividad define las acciones específicas de la sospecha (incluso los pequeños detalles pueden ser importantes más adelante). La ubicación no es sólo la ubicación física de la escena, sino también las posibilidades virtuales del ciberespacio. En términos del ciberespacio puede incluir direcciones de correo electrónico, localizadores de recursos uniformes (URL), nombres de usuario, contraseñas, dominios de red y otros aspectos relacionados, símbolos o las empresas o identificadores de la agencia.

Por último, equipos tratan los diferentes tipos de dispositivos alámbricos e inalámbricos de hardware y aplicaciones de software que se puede esperar cuando se acerque a la escena del crimen digital.
La misión de la investigación se determina normalmente por el tipo de delito cometido, a su vez determinar el nivel de investigación y el nivel de conocimientos necesario para la investigación.

Triage

Una vez que la adecuada planificación se ha completado, el proceso de investigación se traslada a la fase que tiene que ver más directamente con el sospechoso real o escena del crimen (según el caso). Por el bien de la investigación se supone que la escena ha sido debidamente asegurada y controlada. Aquí la escena se refiere tanto a lo físico y lo digital.
Al igual que el tiempo es un factor crucial en CFTTPM, es muy importante que establecer algún tipo de prioridad inicial. En el campo de la medicina triage se refiere a: "Un proceso para la clasificación de heridos en grupos en función de su necesidad o beneficio esperado del tratamiento médico inmediato. Triage se utiliza en salas de emergencia, en campos de batalla, y en lugares de desastres, cuando la escasez de recursos sanitarios ha de ser asignado".
Para nuestros propósitos, triage se defien como: Un proceso en el que las cosas se clasifican en términos de importancia o prioridad. En esencia, esos elementos, piezas de evidencia o recipientes potenciales de la evidencia de que son los más importantes o la necesidad de más volátiles que se abordan en primer lugar.

La fase de clasificación es fundamental para el modelo de proceso y, junto con una planificación adecuada es la base sobre la cual las otras fases se construyen.

Uso / perfiles de usuario

Una vez que los medios de comunicación o un sistema de almacenamiento se ha identificado y priorizado en la fase de triage, al examen y análisis se llevan a cabo. Cuando haya pruebas convincentes y se encuentra en soporte digital, es esencial encontrar una relación entre dichas pruebas y la específica, identificable y suspectib1e.

No siempre es necesario o provechoso evaluar los perfiles de usuario. Al determinar la necesidad y el enfoque más eficiente del tiempo, varias preguntas se deben responder: ¿Cuántas personas utilizan (tener acceso a) la PC? ¿Cuántas cuentas de usuario son? Las respuestas a las dos primeras no son a menudo las mismas, dando lugar a una tercera pregunta, ¿cuántas cuentas o que son compartidas por más de un individuo? Obviamente, en cualquier caso en más de un individuo es capaz de acceder a la misma cuenta, la evaluación de perfiles de usuario en sí mismo, no serán suficientes para establecer la culpabilidad, o incluso el conocimiento de un sospechoso de declarar contra los artefactos. Puede ser necesario el uso de las fechas y horas asociados a artefactos de cargo y ponerlos en contexto con las fechas y horas a un sospechoso tenía acceso a la PC, o existen razones no podía decirse que ha tenido acceso a un PC. Especial cuidado debe tenerse cuando coloque importancia a las fechas y los tiempos de recuperación de evidencia digital.

Directorio de Inicio

De forma predeterminada, el directorio de inicio sólo se puede acceder sólo por la cuenta de usuario asociada. También de forma predeterminada, la ubicación de los archivos almacenados asociados con diferentes aplicaciones se establece en una subcarpeta dentro del directorio de origen. La presencia de documentos de cargo los archivos en el directorio principal del sospechoso o de una de sus subcarpetas (incluyendo personajes notables como "escritorio" mis documentos "y" favoritos ") es un indicador fiable de que sólo el sospechoso (o cualquiera que pueda conectarse a esa cuenta) tenido acceso a esos archivos.

Propiedades de archivo (de seguridad)

Puede ser útil y eficiente del tiempo, destinadas a comprobar la propiedad y las propiedades de seguridad de objetos con valor probatorio conocido. La capacidad de establecer y leer permisos de seguridad no está disponible en FAT, y está desactivado por defecto en Windows, incluso cuando el sistema de archivos NTFS se utiliza. Cuando un archivo es creado, la cuenta de usuario inicia la sesión se registra como el "dueño" como parte del descriptor de seguridad del archivo (Esto se puede cambiar sólo si un administrador de "apropiación" del archivo, en cuyo caso el Administrador se registra como el propietario). Los permisos también pueden ser de utilidad limitada en

el establecimiento de la culpabilidad. Sólo las cuentas que tienen el permiso para hacerlo puede acceder a un objeto, sin embargo esto puede ser una o más cuentas de usuario y las cuentas que tienen permiso para el objeto puede cambiar con el tiempo.

Registro

Aunque la revision del registro puede ser una pérdida de tiempo. Por otro lado, un examinador de conocimiento con una visión clara de la información que desea recuperar puede encontrar varios artículos de gran valor en menos de unos minutos . Por ejemplo, el HKEY_USERSsuspect de SIDSoftwareMicrosoftWindows CurrentVersionExplorer RecentDocs fundamentales y las sub-llaves contienen una lista bastante completa de los archivos que se abrieron, y la cuenta con la fue iniciada la sesión.

Cronología / Línea de tiempo

El alcance cronológico de la investigación puede ser definido por la inteligencia en el caso. En una investigación, la evidencia digital se define por su valor temporal, conocido a veces como MAC .

- ***Modification*** es definido por cuando el contenido de un archivo fue cambiado.
- ***Access time*** es definido por cuando un archivo fue visto.
- ***Created time*** es defindo por cuando un archivo fue creado.

Aunque los tiempos MAC parecen simplse, es bien documentado que hay muchas inconsistencias con los tiempos de MAC y hay varias otras vulnerabilidades al describir otros sistemas de proveedor específico de funcionamiento, tales como los que se utilizan en dispositivos personales de las tecnologías digitales (por ejemplo, PDA's, teléfonos móviles, reproductores de MP3).

Otra cuantificación incluye la identificación y análisis de aplicaciones de software y archivos de datos de acceso y la utilización en tiempos calificados de interés. De nuevo, esto se puede obtener mediante la correlación de usuarios conocidos con los tiempos de MAC posiblemente estableciendo periodos único tiempo que podría ser de gran valor.

Por último, la tercera cuantificación incluye la identificación y análisis de accesos directos reciente y la información almacenada. Estas podrían incluir, pero no se limitan a los elementos en el escritorio, de uso general las aplicaciones de software, y los distintos locales de las cookies del navegador de Internet, la caché y el archivo

index.dat. Tenga en cuenta que las diferentes estructuras de Internet (cookies, caché y el archivo index.dat) puede ser muy útil para determinar la inteligencia cronológico en que estos proporcionan muchaInternet.

Internet

Casi todos los casos será necesario un examen de artefactos asociados con la actividad de Internet, como la mensajería instantánea (IM), correo electrónico y navegación web. El valor, el costo del tiempo, la criticidad y el tiempo puede variar ampliamente, dependiendo de las circunstancias, incluyendo las aplicaciones a las que afecta, tipo de actividad que se examina, y si el PC es examinado como victima o sospechoso.

Objetos del navegador

Aunque los detalles varían, la mayoría de las aplicaciones de navegación web almacenar algún método para almacenar las "cookies", ya sea como un archivo o en archivos separados, algunos medios de almacenamiento de archivos temporales de Internet y algunos medios de información de los usuarios almacenar y preferencias, tales como escrito de recurso uniforme Locator (URL) y "favoritos". El contenido específico de las cookies está determinado por el sitio web de cada individuo, y rara vez de valor probatorio. En la mayoría de los casos, el valor probatorio de una "cookie" se limita a su nombre.

Objetos de correo electrónico

Si la extracción de e-mail es correcta, incluso un examen superficial de todos los e-mail en el buzón de un sospechoso puede tomar muchas horas. Si basado en la web de correo electrónico se utiliza, con frecuencia no hay almacenamiento local de e-mail artefactos.

Objetos de mensajería instantánea

En la mayoría de los casos, esta capacidad de registro está desactivado por defecto, pero pueden, ya menudo se volvió es, por el usuario. La información de contacto para la mayoría de aplicaciones de mensajería instantánea se mantiene en el servidor, y no se puede encontrar en el PC local. Chat registros puede contener una gran cantidad de datos, incluida la propia conversación, así como los nombres de pantalla de otros partidos. Un registro de chat solo puede contener horas de conversación. Un examen detallado de varios registros pueden tener un costo prohibitivo en el tiempo.

Caso Específico

Se trata de un conjunto de habilidades, y requiere la capacidad de conciliar una serie de requisitos en conflicto de la manera más adecuada no sólo para un tipo de caso, pero para configurar cada una de las circunstancias específicas. Existen varias prácticas que pueden facilitar la optimización de los recursos. Un equipo examinador forense debe ser capaz de evaluar los recursos de tiempo, utilizar la inteligencia pre-raid, personalizar objetivos de búsqueda, y dar prioridad a objetivos de búsqueda.

De todos los recursos disponibles para el examinador, el tiempo es generalmente más corto en la oferta. Una cuenta a la hora de tomar acciones es si el requisito de tiempo es "limitada" o "sin límites". El tiempo es claramente la esencial en un caso, pero la falta de un plazo en el caso no acotado puede justificar algunas vías de investigación que no sería viable en una situación delimitada. En todos los casos, el tiempo es un muy costoso. El tiempo de costo de cualquier actividad de control debe ser sopesado en función del potencial de resultados fructíferos de esta actividad.

El valor de la planificación y la inteligencia previa a la operación no puede dejar de enfatizarse. Una información fiable sobre los términos de búsqueda, los contactos, los tipos de actividades, las aplicaciones usadas, etc antes de que la búsqueda se puede permitir que el examinador a desarrollar por lo menos algunas de las estrategias de búsqueda antes de la llegada a la escena.

3.1.4. Modelo Básico de Análisis Forense

El Modelo básico de Análisis Forense, que se utilizara para responder un incidente presenta las siguientes fases:

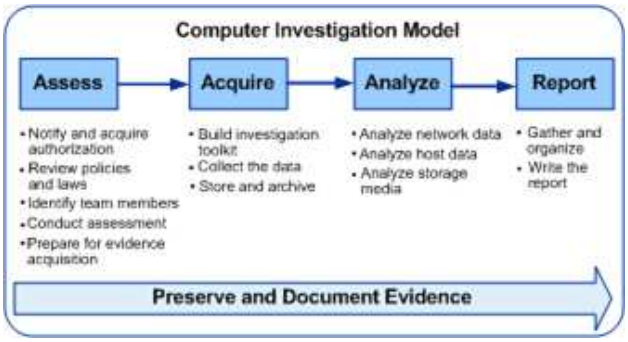


Figura III.12. Diagrama de Modelo Básico de análisis forense

Identificación:

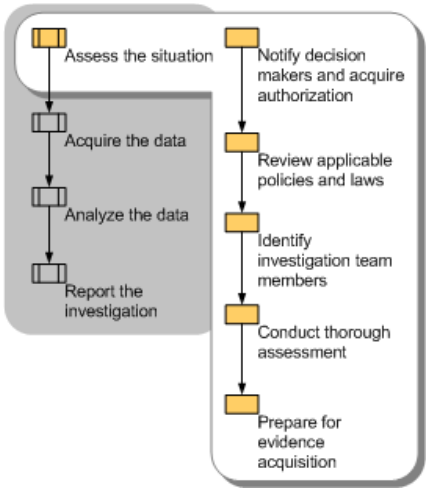


Figura III.13. Fase de Identificación

- En esta fase se realiza una evaluación de los recursos, alcance y objetivos necesarios para realizar la investigación interna.
- Obtener por escrito la autorización para iniciar la Forense (Investigación de equipos). Acuerdos de confidencialidad.
- Documentarse de todas las acciones y antecedentes que preceden la investigación. Los acontecimientos y decisiones que se adoptaron durante el incidente y su respuesta al incidente. La cual determinara el curso de acción a seguir en la Investigación.
- Organizar y definir el Team de Investigación, estableciendo Limites, funciones y responsabilidades.
- Realiar una investigación preliminar (documentación) que le permita describir la situación actual, hechos, las partes afectadas, posibles sospechosos, gravedad y criticidad de la situación, infraestructura afectada, para lograr una compresión total de la situación actual del incidente y definir un curso de acción acorde a la situación.
- Identificar el impacto y la sensibilidad de la información (de clientes, financieros, comerciales, de Investigación y Desarrollo, etc)
- Analizar el impacto de los negocios através de la investigación del Incidente. Como, tiempos de inactividad, costos de equipos afectados o dañados, perdida en ingresos,

costos de recuperación, perdida de informacion confidencial, perdida de credibilidad e imagen, etc.

- Identificar la topologia de red y tipologia de red, equipos afectados (servidores, aplliance, UMT, estaciones, Sistemas Operativos, Router, Switches, IDS's, etc)
- Identificar los dispositivos de almacenamiento o elementos informáticos (Discos Duros, Pen drive, memorias, tarjetas flash, Tapes, Zip Disk, Opticos, Disquettes, Cds, Dvd, etc) que se consideren comprometidos y sean determinados como evidencia, su marca, modelo, caracteristicas, seriales, etc.
- Identificar los posibles implicados o funcionarios que tengan relación con la investigación y efectuar entrevistas, con usuarios o administradores responsables de los sistemas, documentar todo y tratar de lograr un conocimiento total de la situación.
- Realizar una recuperación de los logs de los equipos de comunicación y dispositivos de red, involucrados en la topología de la red.

El producto final de esta fase, debe entregar un documento detallado con la información que permita definir un punto de inicio para la adquisición de datos y para la elaboración del documento final.

Inicia la cadena de Custodia, llenando el formato correspondiente, iniciando una bitácora de los procesos que se llevan a cabo y el embalaje de la Evidencia.

Determinar: **Quien?, Que?, Donde?, Por qué? Mantener una copia con la evidencia, Como?, Cuando?**

- Quien es el primero en tener la evidencia?
- Donde, cuando y quien es el primero que tiene la evidencia
- Donde, cuando y quien examino la evidencia
- Quien va a tener custodia de la evidencia y por cuanto tiempo la tendrá
- Quien y como se embalo y almaceno la evidencia
- Cuando se realiza el cambio de custodia y como se realiza la transferencia

Adquisición:

En esta segunda fase, procedemos a ejecutar los 3 pasos que visualizamos en el gráfico anterior para adquirir la evidencia sin alterarla o dañarla, se autentica que la información de la evidencia sea igual a la original.

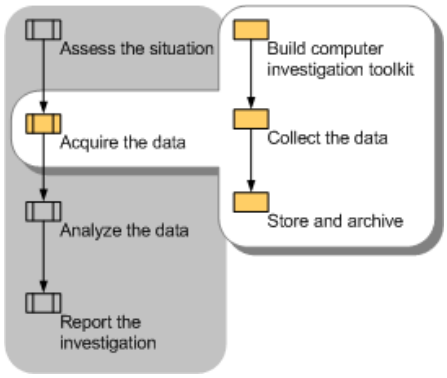


Figura III.14. Fase de Identificación

Se debe definir los equipos y herramientas determinadas para llevar a cabo la investigación. Lograr un entorno de trabajo adecuado para el análisis y la investigación. Iniciar una Bitácora, que permita documentar de manera precisa e identificar y autenticar los datos que se recogen, tipo:

- ¿Quién realiza la acción y por qué lo hicieron.
- ¿Qué estaban tratando de lograr?
- ¿Cómo se realiza la acción, incluidas las herramientas que utilizaban y los procedimientos que siguieron?
- Cuando se realizó la acción (fecha y hora) y los resultados.

De igual forma, se toman otras fuentes de información de los sistemas vivos, los datos volátiles como:

- Cache del Sistema
- Archivos temporales
- Registros de sucesos.
- Registros de internos y externos que los dispositivos de red, tales como firewalls, routers, servidores proxy,etc.
- Logs del sistema, Aplicaciones.

- Tablas de enrutamiento (arp, cache de Netbios, lista de procesos, informacion de la memoria y el kernel)
- Registros remotos e información de monitoreo relevante

Realizar copia imagen de los dispositivos (bit a bit), con una herramienta apropiada y firmar su contenido con un hash de MD5 o SHA1, generando así el segundo original, a partir de este se generaran las copias para el Análisis de datos, cada copia debe ser comprobada con firmas digitales nuevamente de MD5 o SHA1. Documente la evidencia con el documento del embalaje (y cadena de custodia) que puedan garantizar que se incluye información acerca de sus configuraciones. Por ejemplo, anote el fabricante y modelo, configuración de los puentes, y el tamaño del dispositivo. Además, tenga en cuenta el tipo de interfaz y de la condición de la unidad.

Importante considerar las buenas prácticas para conservar la información y la evidencia. Asegurar de manera física un lugar para almacenar los datos, evitando su manipulación. No olvide documentarlo.

- Proteger los equipos de almacenamiento de los campos magnéticos (estática).
- Realice mínimo el segundo original y una copia del segundo original para el análisis y almacene el segundo original en un sitio seguro
- Asegurar que la evidencia está protegido digital y físicamente (por ejemplo, en una caja fuerte, asignar una contraseña a los medios de almacenamiento). Nuevamente, no olvide actualizar el documento de Cadena de custodia (incluye información como el nombre de la persona que examina la evidencia, la fecha exacta y el tiempo que echa un vistazo a las pruebas, y la fecha exacta y hora en que lo devuelva).

Se pretende que esta información sea:

- Autentica
- Correcta
- Completa
- Convincente
- Para que en caso de un proceso sea legal, admisible.

Análisis de Datos:

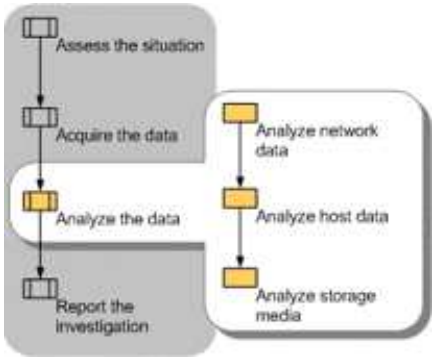


Figura III.15. Fase de Análisis del Modelo Básico

Seguiremos los tres pasos de la anterior figura:

Análisis de Datos de la Red:

Se debe identificar los dispositivos de comunicación y de defensa perimetral (Servidores Web, Firewall, IDS's, IPS's, Proxys, Filtros de Contenido, Analizadores de Red, Servidores de Logs,etc.) que están en la Red, con la finalidad de recuperar los logs que se han tomado como parte de la gestión de red.

Análisis de los Datos del Host:

Generalmente se logra con la información obtenida de los sistemas vivos, de la lectura de las Aplicaciones y los Sistemas Operativos. Se debe limitar a tratar de recuperar estos archivos de la evidencia en procesos de Data Carving o Recuperación de Datos, y definir criterios adecuados de búsqueda, debido a que lo más probable es que se encuentre una gran cantidad de información que puede complicar o facilitar el análisis de datos, dependiendo de los objetivos de búsqueda.

Análisis de los Medios de Almacenamiento:

Igual que el punto anterior s debe definir criterios de búsqueda con objetivos claros, debido a la gran cantidad de información disponible, que puede desviar la atención o sencillamente complicar el proceso de análisis de la información se debe tener en cuenta las buenas prácticas:

- No olvidarse, que se debe utilizar la copia del segundo original, a su vez el segundo original preservarlo manteniendo un buen uso de la cadena de custodia.

- Determinar si los archivos no tienen algún tipo de cifrado (varias claves del registro no lo pueden determinar).
- Preferiblemente descomprimir los archivos con sistemas de compresión
- Crear una estructura de Directorios y Archivos recuperados.
- Identificar y recuperar los archivos objetivo (determinados por algunos criterios, ejemplo aquellos que han sido afectados por el incidente). Y se puede comparar su hash (archivos del sistema operativo y aplicaciones) con los hash de archivos que nos facilita la http://www.nsrl.nist.gov/, O sitios como:http://www.fileformat.info/resolución/web/filespecs/index.htm, http://www.wotsit.org/, http://www.processlibrary.com/
- Analizar archivos de Booteo y configuración del sistema, el registro del sistema
- Información de Login/Logout del sistema, nombres de usuario e información del AD (Directorio Activo)
- Software instalado, actualizaciones y parches.
- Buscar archivos con NTFS ADS (Alterna Data Stream)
- Estudio de las Metadata (en especial identificar las marcas de tiempo, creación, actualización, acceso, modificación,etc).
- La evidencia debe ser cargada de solo lectura, para evitar daños o alteraciones sobre las copias del segundo original.

Preparación del Informe

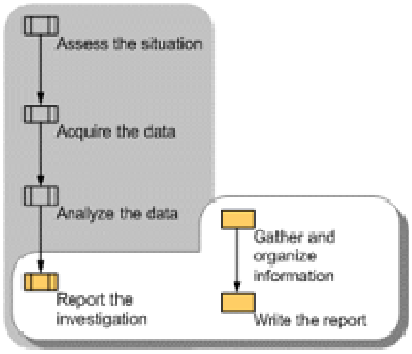


Figura III.16. Fase de Identificación del Modelo Básico

Es la fase final y la más delicada e importante la cual será el documento que sustentara una prueba en un proceso legal, básicamente tener en cuenta estos dos pasos:

Organización de la Información:

Retomemos toda la documentación generada en las fases de la metodología e igual cualquier información anexa como notas, antecedentes o informe policial.

Identifiquemos lo más importante y pertinente de la investigación

Realizar conclusiones (tenga en cuenta los hechos) y crear una lista de las pruebas para presentar.

Escribir el Informe Final:

Debe ser claro, conciso y escrito en un lenguaje entendible para gente común (no tan técnico).

Debe contener como mínimo:

Propósito del Informe. Explicar claramente el objetivo del informe, el público objetivo, y por qué se preparó el informe.

Autor del informe. Todos los autores y co-autores del informe, incluyendo sus posiciones, las responsabilidades durante la investigación, y datos de contacto.

Resumen de Incidentes. Introducir el incidente y explicar su impacto. El resumen deberá estar escrito de manera que una persona no técnica, como un juez o jurado sería capaz de entender lo que ocurrió y cómo ocurrió.

Pruebas. Proporcionar una descripción de las pruebas de que fue adquirido durante la investigación. Cuando el estado de la evidencia que describen la forma en que fue adquirida, cuándo y quién lo adquirió.

Detalles · Proporcionar una descripción detallada de lo que la evidencia se analizó y los métodos de análisis que se utilizaron. Explicar los resultados del análisis. Lista de los procedimientos que se siguieron durante la investigación y de las técnicas de análisis que se utilizaron. Incluir una prueba de sus resultados, tales como los informes de servicios públicos y las entradas de registro. Justificar cada conclusión que se extrae del análisis. Sello documentos de apoyo, el número de cada página, y se refieren a ellos por el nombre de la etiqueta cuando se examinan en el análisis. Por ejemplo, “registro de Firewall de servidor, documento de apoyo D.” Además, proporcionan información

sobre aquellos individuos que realizaron o participaron en la investigación. Si procede, proporcione una lista de testigos.

Conclusión. Resumir los resultados de la investigación. La conclusión debe ser específica de los resultados de la investigación. Citar pruebas concretas para demostrar la conclusión, pero no dan excesivos detalles acerca de cómo se obtuvieron las pruebas (tal información debe estar en la sección “Detalles”). Incluir una justificación para su conclusión, junto con las pruebas y la documentación. La conclusión debe ser lo más clara y sin ambigüedades como sea posible. En muchos casos, se declaró cerca del comienzo del informe, porque representa la información procesable.

Los documentos justificativos. Incluir cualquier información de antecedentes a que se refiere en todo el informe, tales como diagramas de red, los documentos que describen los procedimientos de investigación de equipos usados, y un panorama general de las tecnologías que intervienen en la investigación. Es importante que los documentos justificativos proporcionar información suficiente para que el lector del informe para comprender el incidente tan completamente como sea posible. Como se mencionó anteriormente, la etiqueta de cada documento de apoyo con las letras y el número de cada página del documento. Proporcionar una lista completa de los documentos justificativos.

Si es probable que el informe sea presentado a un público variado, considerar la creación de un glosario de términos utilizados en el informe. Un glosario es especialmente valiosa si el organismo de aplicación de la ley no está bien informado sobre cuestiones técnicas o cuando un juez o jurado debe revisar los documentos.

En la siguiente tabla se lista las fases o pasos de los cuatro modelos y se indica con un visto la fase que pertenece a cada modelo respectivamente.

Tabla III.IV Cuadro resumen de los modelos de análisis forense de acuerdo a sus fases o pasos

Modelo	Modelo Digital Forensic Research Workshops (DFRW)	Modelo Forense Digital Abstracto	Modelo CFFTPM	Modelo Básico de Análisis Forense
Preparación	√	√	√	√
Planificación			√	
Asegurar la escena	√		√	√
Estudio y reconocimiento	√		√	√
Documentación de la Escena	√			√
Colección de Evidencia Volátil	√	√	√	√
Colección de Evidencia No Volátil	√	√	√	√
Examen de Datos		√	√	
Preservación	√	√	√	
Análisis	√	√	√	√
Presentación	√	√		√
Revisión		√		
Decisión	√			
Suma	**10**	**8**	**9**	**8**
Total (%)	**76.92%**	**61.54%**	**69.23%**	**61.54%**

Fuente: Análisis práctico realizado en la tesis

Elaborado por: Ana Juntamay

Tabla III.V Definición de parámetros

PARÁMETRO	DEFINICIÓN
Considera Todo el Sistema	Analiza todos los elementos del sistema de forma completa (S.O, Memoria, Red, etc.)
Guardar la información de registro	Se almacena la información adquirida de los registros analizados.
Presentar los eventos de manera en que puedan ser analizados y entendidos	Mantiene un orden y seguimientos de los eventos de forma y concisa para su posterior revisión.
Posee sub- tareas o pasos dentro de cada Fase	Se refiere a que la fase puede dividirse en sub- tareas o pasos para mejorar el proceso.
Determina Herramientas Software en alguna Fase	Se refiere a que el modelo puede sugerir la utilización de herramientas software en alguna de sus fases.
Define como realizar el Informe Final a entregar	Le indica al perito un formato de cómo realizar el Informe Final.

Fuente: Análisis práctico realizado en la tesis

Elaborado por: Ana Juntamay

Tabla III.VI Cuadro resumen de los modelos de análisis forense

Modelo	Modelo Digital Forensic Research Workshops (DFRW)	Modelo Forense Digital Abstracto	Modelo CFFTPM	Modelo Básico de análisis forense
Considera todo el sistema	√	√	√	√
Guardar la información de registro	√	√	√	√
Presentar los eventos de manera en que puedan ser analizados y entendidos			√	√
Posee sub-tareas o pasos dentro de cada Fase			√	√
Determina Herramientas Software en alguna Fase		√		√
Define como realizar el Informe Final a entregar				√
Suma	**2**	**3**	**4**	**6**
Total (%)	**33.33%**	**50%**	**66.67%**	**100%**

Fuente: Análisis práctico realizado en la Tesis

Elaborado por: Ana Juntamay

De acuerdo a las tablas resumen anteriormente expuestas se puede concluir que el modelo básico forense es el que cumple con la mayoría de parámetros propuestos en esta investigación, y se identifica claramente que es el modelo más completo y que considera todo el sistema afectado para evitar la pérdida o contaminación de la evidencia digital.

CAPÍTULO IV

ESTUDIO DE HERRAMIENTAS SOFTWARE

4.1. INTRODUCCIÓN

En este capítulo se va revisar las herramientas software que permiten reparar o recuperar los archivos dañados en MySQL 5.x y en SQL Server 2005, así también las herramientas de detección de vulnerabilidades en una base de datos y las herramientas forenses que nos permitan recolectar la evidencia digital de manera más fácil y ágil.

A continuación se expone un cuadro resumen de las herramientas software que se analizaron dependiendo de su funcionalidad y que serán utilizadas en la presente investigación.

Tabla IV.VII Cuadro Resumen de Herramientas Software

HERRAMIENTAS SOFTWARE
Detección de Vulnerabilidades • Acunetix Web Vulnerability Scanner • Havij • NGSSQuirrel • N-Stalker • SQLRecon • WebCruiser
Reparación y Recuperación • Recovery For My Sql • Acronis Recovery For Ms Sql Server • Stellar Phoenix Database Recovery For Mysql • Systools Sql Recovery • Stellar Phoenix Sql Recovery • Recovery For Sql Server
Herramienta para proceso de Análisis Forense • Helix Live CD • SQL Server Managemen Studio Express • SQLCMD • Windows Forensic Toolches • MD5SUM

Fuente: Análisis práctico realizado en la Tesis
Elaborado por: Ana Juntamay y Nancy Macas

4.2. HERRAMIENTAS DE DETECCIÓN DE VULNERABILIDADES

Luego de lo anteriormente expuesto se tiene una idea general respecto a la problemática en torno a la seguridad en base de datos y entre otras se conoce que el software de base de datos, es igual que cualquier otro tipo de software, que permite al atacante la posibilidad de explotar vulnerabilidades propias de este tipo de aplicaciones. Por tanto, es conveniente que los servidores de base de datos sean asegurados y testeados.

A continuación se presenta las herramientas software más representativas que existen en la actualidad teniendo en cuenta que las licencias de estas son trial, ya que su costo es muy elevado para su adquisición.

ACUNETIX WEB VULNERABILITY SCANNER

Definición

Acunetix es una herramienta diseñada para descubrir agujeros de seguridad en sus aplicaciones web, que un atacante hace abuso de probabilidades de aumentar el acceso ilícito a sistemas y datos. Busca vulnerabilidades múltiples, incluyendo la inyección SQL, cross site scripting, y contraseñas débiles.

La aplicación puede ser utilizada para realizar escaneo de vulnerabilidades web y de aplicaciones y para realizar la penetración las pruebas en contra de los problemas identificados. Sugerencias de mitigación son provistas a la sazón cada debilidad y se puede utilizar para aumentar la seguridad del servidor web o una aplicación se está probando.

Características

- Permite localizar y corregir la vulnerabilidad más rápido debido a la capacidad de proporcionar más información acerca de la vulnerabilidad, tales como número de línea del código fuente, seguimiento de pilas, la consulta SQL afectada, etc.
- Pueden reducir los falsos positivos al analizar un sitio Web porque podemos internamente comprender mejor el comportamiento de la aplicación web.
- Puede alertar de problemas de configuración de aplicación web que podrían dar lugar a una aplicación vulnerable o exponer los detalles de la aplicación interna. Por ejemplo, si errores personalizados están habilitados en. NET, esto podría exponer detalles sensibles de la aplicación a un usuario malintencionado.
- Detecta muchas más vulnerabilidades de inyección SQL. Anteriormente sólo podía encontrar vulnerabilidades de inyección de SQL si se informaba de errores de la base de datos o a través de otras técnicas comunes.
- Detecta las vulnerabilidades de inyección SQL en todas las instrucciones SQL, incluyendo en declaraciones SQL INSERT. Con un escáner de caja negra no pueden encontrarse dichas vulnerabilidades de inyecciones SQL.

- Capacidad de saber acerca de todos los archivos presentes y accesibles a través del servidor web. Si un atacante obtiene el acceso al sitio Web y crea un archivo de puerta trasera en el directorio de la aplicación, el archivo será encontrado, se analizará cuando se utiliza la tecnología AcuSensor y se te avisará.
- No hay necesidad de escribir la dirección URL con sus reglas al análisis de las aplicaciones web que utilizan un motor de búsquedas URL amigables, mediante la tecnología de AcuSensor el escaneador es capaz de volver a escribir direcciones URL SEO sobre la marcha.
- Capacidad para probar las vulnerabilidades de creación y eliminación del archivo arbitrario. Por ejemplo, a través de una escritura vulnerable malintencionada el usuario puede crear un archivo en el directorio de la aplicación web y ejecutarlo para que tenga acceso privilegiado o para que elimine archivos importantes de la aplicación web.
- Capacidad para probar las inyecciones del correo electrónico. Por ejemplo, un usuario malintencionado puede anexar información adicional tal como una lista o algunos destinatarios o información adicional al cuerpo del mensaje para enviarlo bajo un formulario web o a un gran número de destinatarios como spam de forma anónima.

Utilidad

Acunetix es una herramienta fácil de utilizar puede trabajar con el asistente de escaneo, en la primera ventana le pide que ingrese la dirección URL a la que va a escanear.

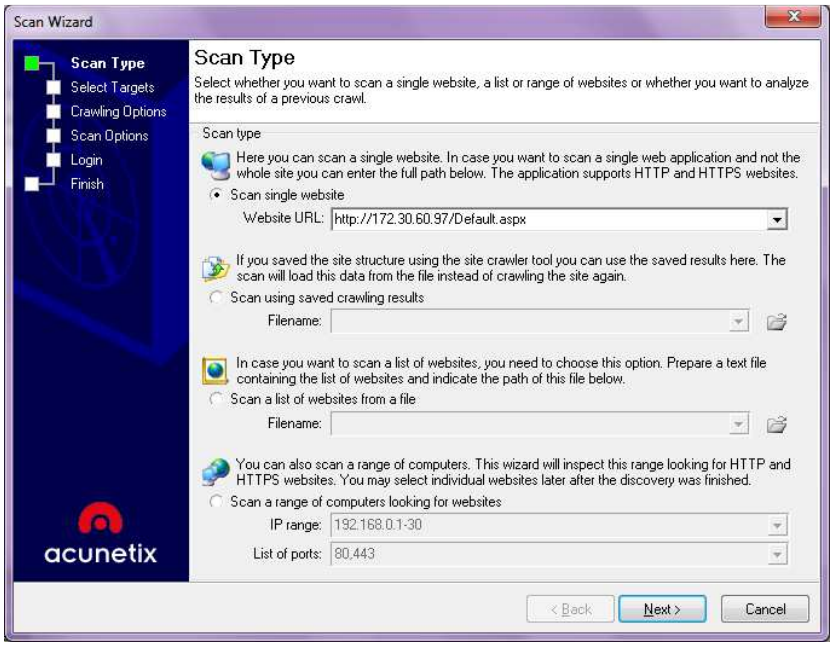


Figura IV.17. Tipo de Escaneo de Acunetix Web Scanner

En esta pantalla se observa información del servidor web y del sistema operativo que está usando el sitio web a escanear.

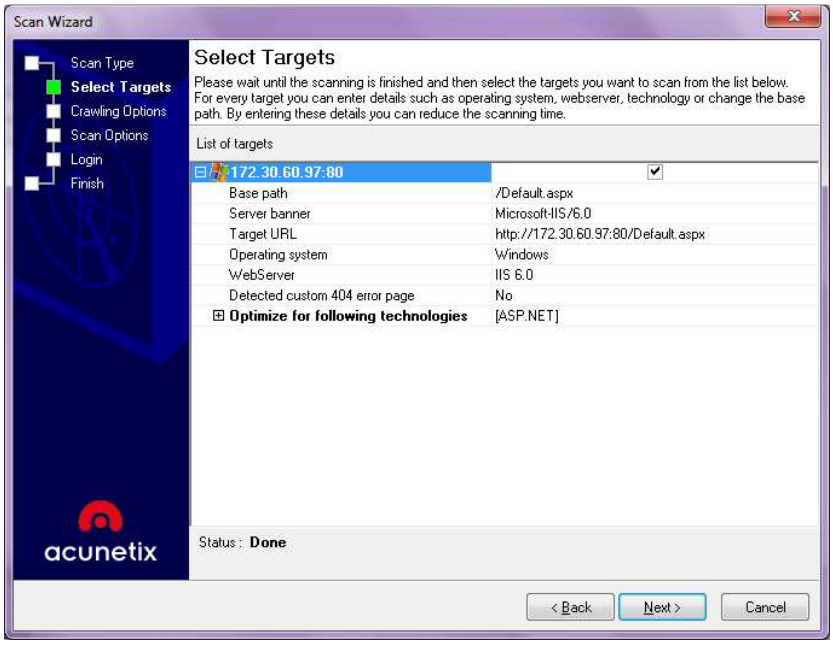


Figura IV.18. Seleccionar el target para el escaneo

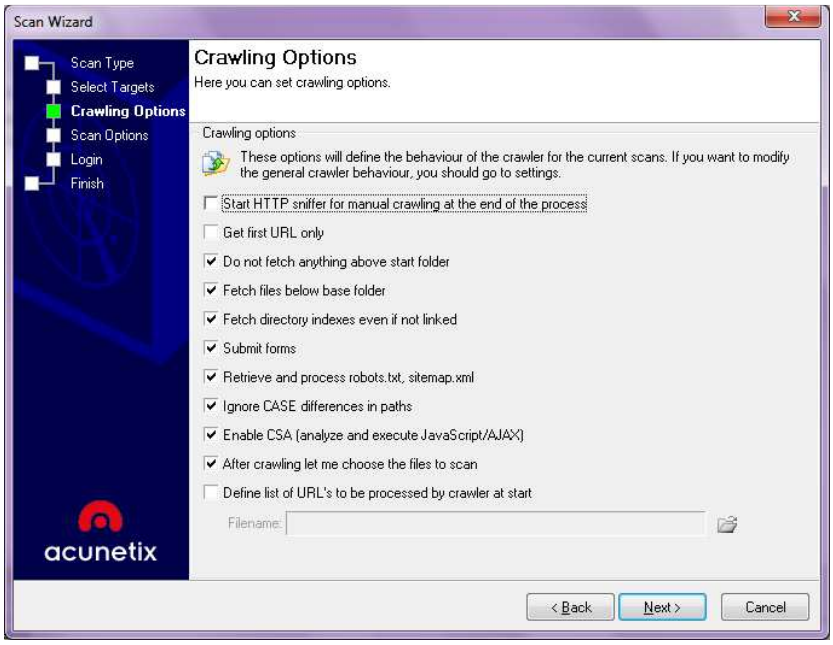


Figura IV.19. Seleccionar opciones para el escaneo

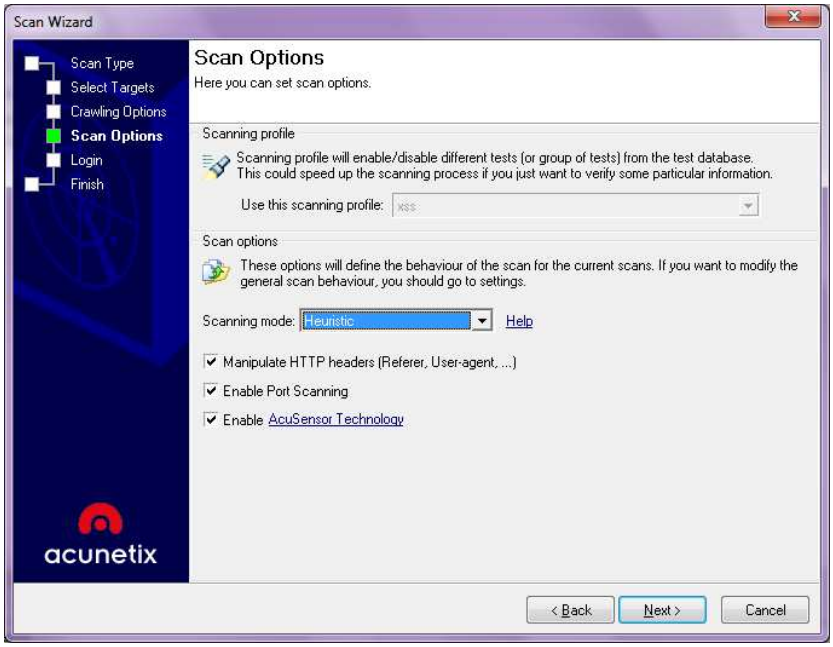


Figura IV.20. Seleccionar el modo de escaneo

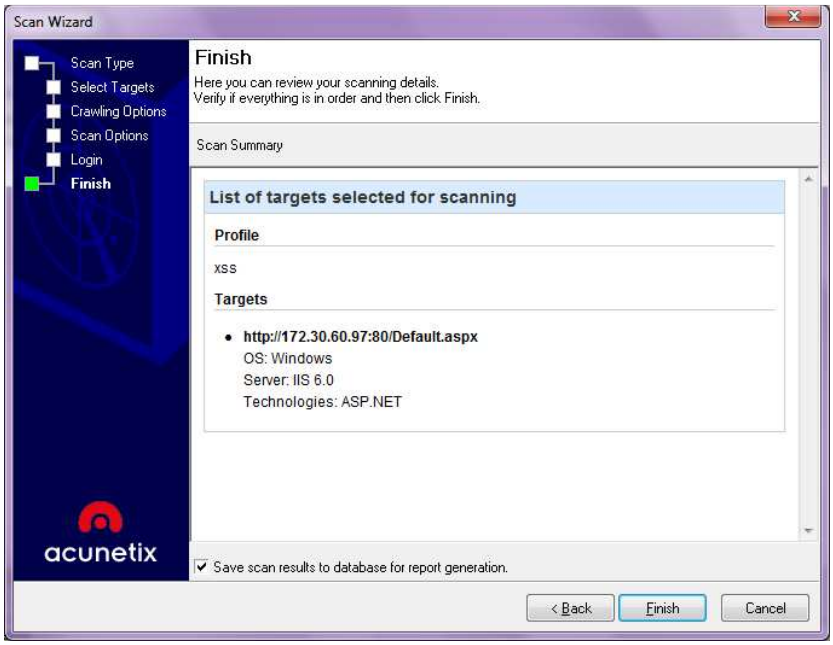


Figura IV.21. Finalización de Escaneo

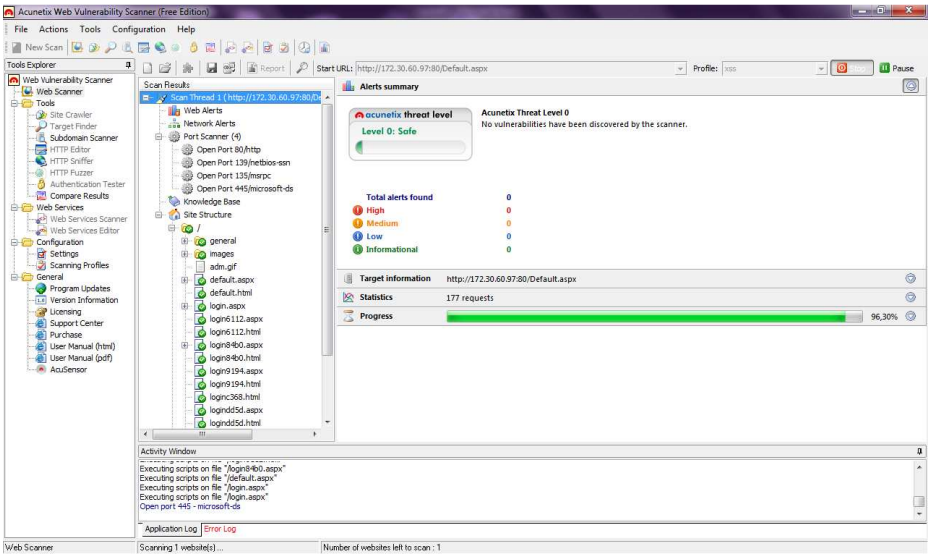


Figura IV.22. Resultados de Escaneo

HAVIJ

Definición

Havij es una herramienta gratuita programada en Visual basic, la cual permite automatizar la inyección SQL y ayuda a los probadores de penetración a encontrar vulnerabilidades en una página web y explotar la inyección SQL. Todo lo que necesita

saber un poco de inyección de SQL y ya está. Usted sólo necesita hacer clic en un botón y esperar hasta que encuentra una explotación de consulta SQL. No sólo eso, también puede buscar una base de datos, recuperar usuarios DBMS y los hashes de contraseñas, tablas y columnas de descarga, ir a buscar los datos de la base de datos, ejecuta las sentencias SQL, e incluso acceder al sistema de archivos subyacente y la ejecución de comandos en el sistema operativo.

Características

Estas son las funciones actuales que Havij aporta a partir de ahora:

- Posee detección automática de la base de datos
- Soporta una amplia gama de bases de datos - MSSQL, MySQL, MS Access y Oracle.
- Puede evadir la detección de IDS por un simple pre-configurado y trucos de esta herramienta.
- Detección automática de tipo (cadena o un entero)
- Detección automática de palabras clave (la diferencia entre encontrar la respuesta positiva y negativa)
- Adivinar tablas y columnas en mysql <5
- Obtención de información del DBMS
- Obtención de tablas, columnas y datos
- Ejecución de comando (mssql solamente)
- Lectura de archivos de sistema (mysql solamente)
- Insertar, actualizar o borrar datos

Utilidad

Para esta herramienta se utiliza un sitio web en php y mysql en target copie la dirección URL y dar clic en Analyze y le muestra la siguiente información.

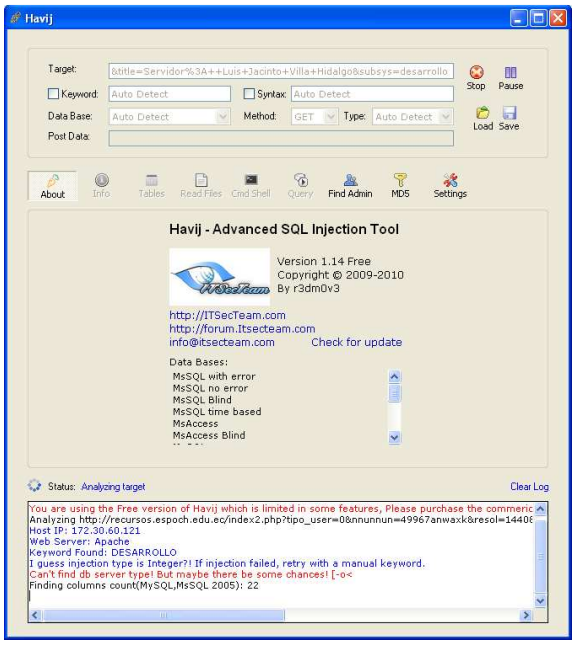


Figura IV.23. Resultados de Escaneo con Havij y la opción Autodetect

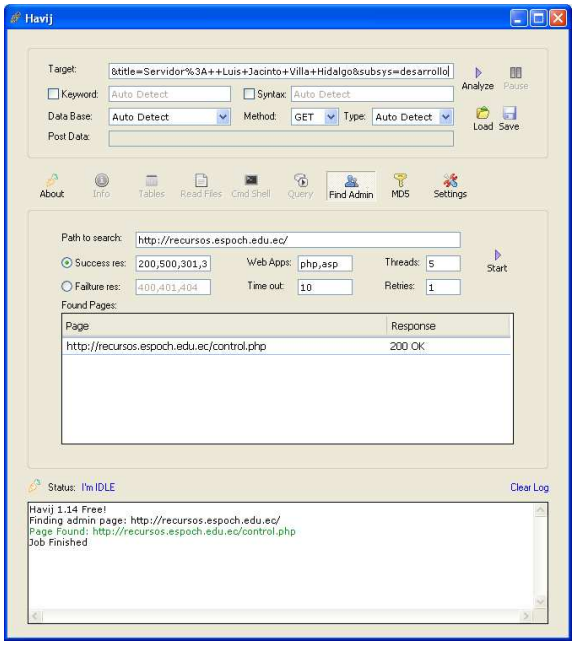


Figura IV.24 Opción Find Admin

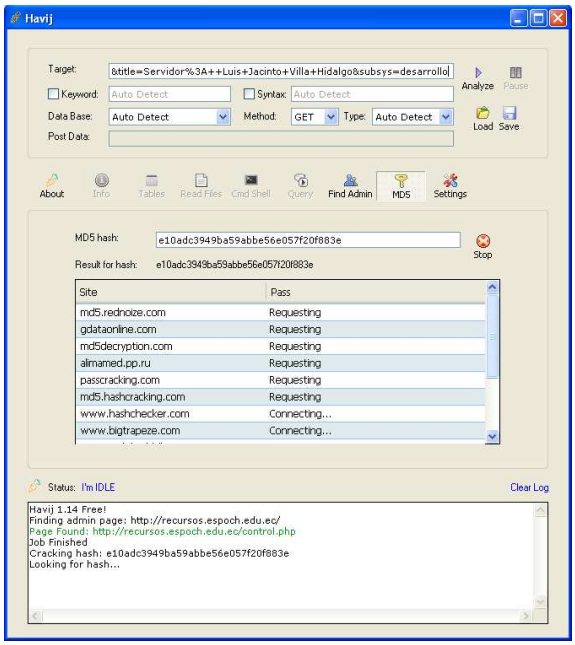


Figura IV.25. Opción MD5 en Havij

En la siguiente ventana se realiza la inyección SQL denominada MySQL Blind y obtiene la dirección IP del Servidor, el Servidor Web que usa y la palabra clave, pero no pudo realizar con éxito la inyección SQL al sitio por su la seguridad que posee.

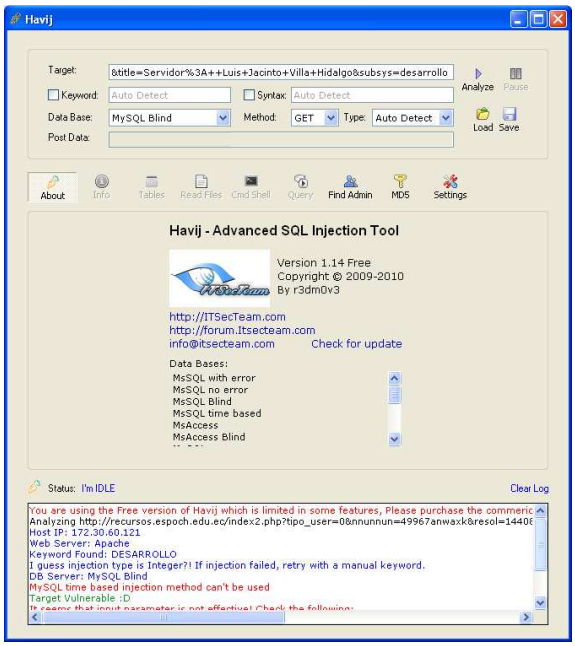


Figura IV.26. Opción MySQL Blind a un sitio web

NGSSQUIRREL

Definición

NGSSQuirrel es una herramienta de gestión para Microsoft SQL Server que puede generar automáticamente una secuencia de comandos de bloqueo basado en las vulnerabilidades encontradas, además de ejecutar una auditoría de seguridad completa. La aplicación de este software le ayudará a proteger el servidor contra hackers y robo de datos no autorizados. De esta manera NGSSQuirrel facilita enormemente la carga administrativa de las acciones de protección de servidores SQL Server.

Características

- Comprueba arquitectura de una nueva base de datos para la visualización y edición de controles básicos, controles de creación de usuario, las referencias de usuarios y tipos de usuarios de referencia.
- Security Manager administra y gestiona los inicios de sesión, funciones, bases de datos y procedimientos almacenados extendidos.
- Controla procedimientos almacenados
- Un clic en soluciones para las vulnerabilidades mediante la generación de secuencias de comandos de bloqueo.
- Exploración flexible por la selección manual de los grupos de verificación para ejecutar y una opción para ver todos los controles realizados
- Los controles para la puesta en marcha de procedimientos y contraseñas débiles
- La información en un archivo de texto, RTF, XML, HTML (estática o dinámica) y la base de datos externa
- Compatible con versiones de SQL Server 7, 2000, 2005 y 2008

Utilización

Al abrir la herramienta se muestra la siguiente ventana asistente.

Figura IV.27. Ventana del Asistente de NGSSQuirrel

Ahora en esta ventana nos pide que ingrese la dirección IP del Servidor de Base de Datos que desea escanear y el puerto que este caso el programa lo pone por defecto.

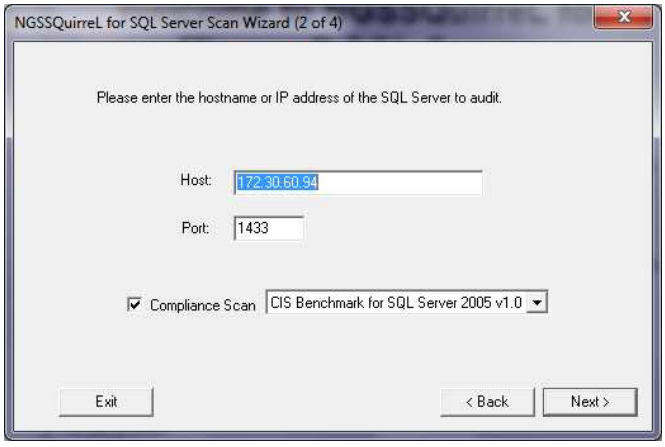


Figura IV.28. Ingreso de la dirección IP de SQL Server

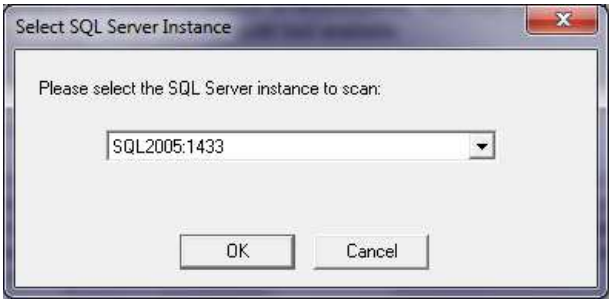


Figura IV.29. Seleccionar la instancia de SQL Server

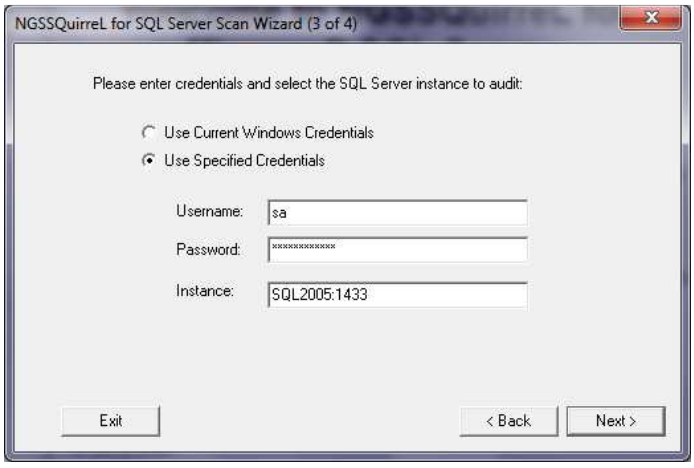


Figura IV.30. Ingresar credenciales SQL Server

Ahora se muestra todos los datos previamente establecidos para iniciar el escaneo del Servidor de Base de Datos.

Figura IV.31. Información de SQL Server por NGSSQuirrel

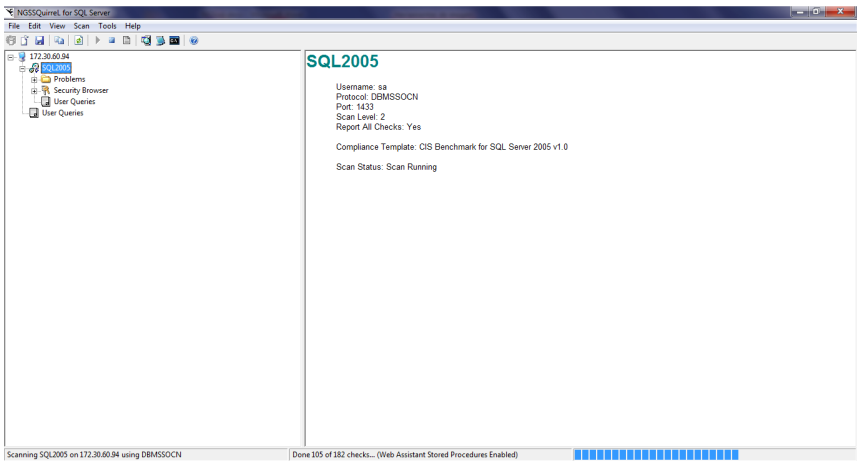


Figura IV.32. Información de SQL Server 2005 por NGSSQuirrel

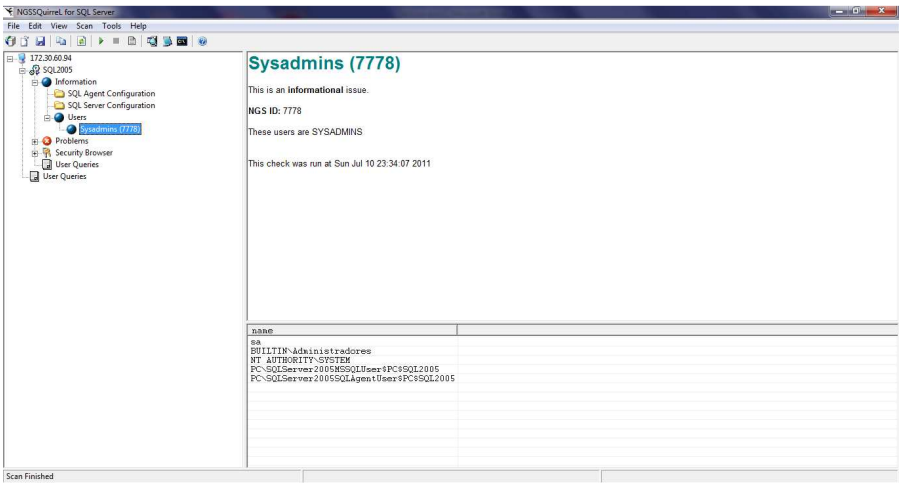


Figura IV.33. Usuarios de SQL Server

En esta ventana se observa las vulnerabilidades que detecta en el Servidor de Base Datos.

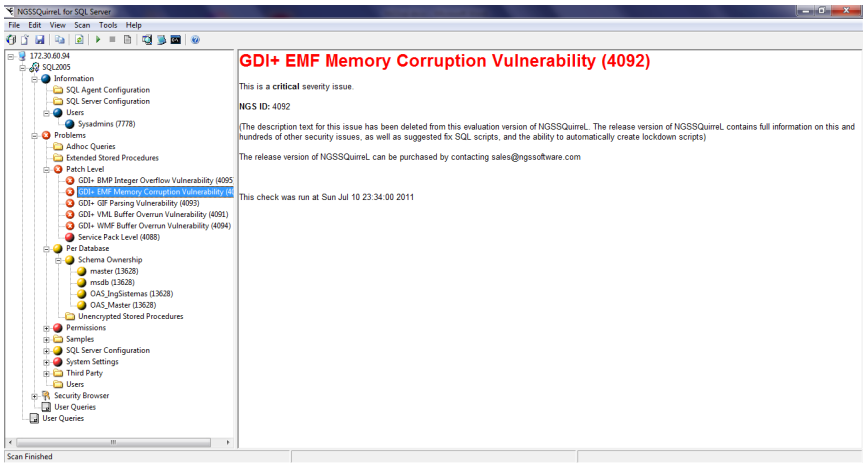


Figura IV.34. Problemas de SQL Server detectadas por NGSSQuirrel

N-STALKER

Definición

La N-Stalker Web Application Security Scanner fue creado en abril de 2000 por especialistas en seguridad informática, que evalúa una aplicación web contra una amplia variedad de vulnerabilidades, incluyendo la capa de aplicación y la capa de infraestructura. Analiza en busca de la capa de aplicación se basan en la Open Web Application Security Project (OWASP) Top 10 y comunes.

Este producto es muy fácil de instalar, pero un poco difícil de usar. Después de que la aplicación este instalada, todo se ejecuta desde la aplicación N-Stalker. Esta aplicación tiene un aspecto limpio y organizado, pero puede ser un poco abrumador al principio. Este producto tiene una gran cantidad de opciones que se pueden configurar, así que se debe dedicar unos minutos a familiarizarse con la consola.

Características

- Permite opciones a configurar, tales como la elección de la meta y la optimización de la configuración para hacer frente a la autenticación y falsos positivos.
- Durante una exploración, el Web Application Security Scanner debe enviar el tráfico del explorador-como hacia el objetivo, pero no depende de ninguna aplicación externa. Todo esto se hace a través de la única aplicación independiente.
- La documentación incluye una única guía de usuario en PDF, que cubre todo el producto de la instalación mediante el uso de características y configuración avanzada.
- Prevención automática del motor de falsos positivos
- Pruebas de evasión de IDS fuzzing
- Ataque Especial de la consola para explorar las vulnerabilidades.
- Soporte a múltiples esquemas de autenticación, incluyendo formulario Web, HTTP y la autenticación X.509.
- Informe Final soporta varios formatos (RTF, PDF)

Utilidad

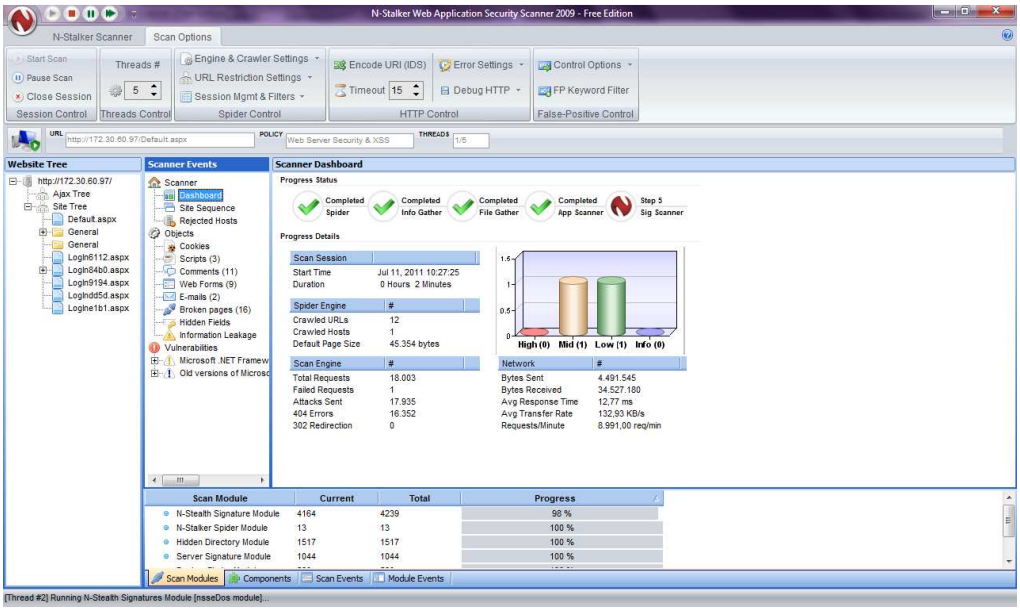


Figura IV.35. Resultados de Escaneo con N-Stalker

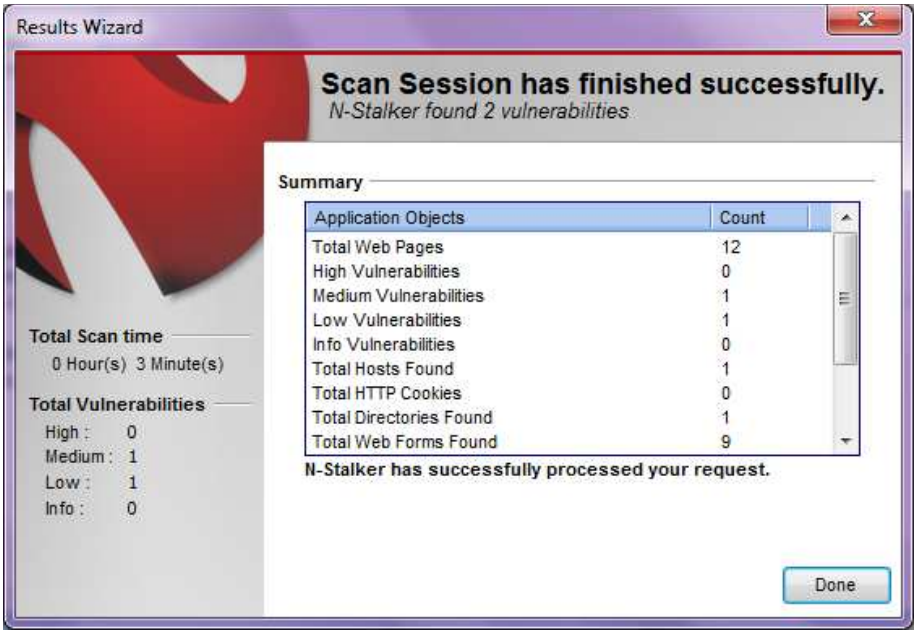


Figura IV.36. Finalización de escaneo de N-Stalker

SQLRECON

Definición

Es una potente herramienta que de forma automática, permite entre otras funciones, descubrir bases de datos tipo MS-SQL. Esta dirigida a ofrecer a los administradores agobiados dentro de grandes redes, un sistema fácil para descubrir si alguien hace procesos inadecuados como por ejemplo, la instalación de un servidor sin permisos jerárquicos, comprobando de paso si existe el usuario SA y si su contraseña es nulo o no, como cuando se instala por defecto un servidor MS-SQL.

Puede explorar la red mediante las siguientes técnicas:

UDP (por sondeo UDP 1434)

REG (control de registro remoto)

WMI: (iniciar una consulta de WMI)

TCP: (scaning puerto TCP 1433 por defecto el puerto TCP para SQL Server y MSDE/ 'puerto del servidor Ocultar' 2433)

SMC: (consultar el administrador de control de servicios)

SA: (acceso a la instancia de SQL Server con una contraseña en blanco)

BRO: (control al servicio del navegador para SQL registro de Server)

AD: (consulta de Active Directory de registro de servidores SQL Server)

Características

- Motor de escaneo Multi-threaded
- 6 Técnicas de Escaneo Active
- Escaneo de rangos de IP
- Escaneo de Lista IP
- Exportar resultados como XML o un archivo de texto
- Exportar lista IP para un futuro escaneo
- Revisar ICMP para incrementar velocidad de escaneo
- Modo Debug que permite mejorar la visibilidad de escaneo
- Permite credenciales alternativas
- Personalización de Puerto de origen UDP para evasión de firewall

Utilidad

Su funcionamiento es sencillo, una vez descargada e instalada, la ejecutaremos ingresando tan solo la dirección IP de nuestro servidor objetivo, en los campos mencionados como Start/End dentro del cuadro "IP Range". Luego tan solo presionaremos "Scan" y esperaremos los resultados.

En este caso en particular y tan solo para remarcar el valor agregado de esta herramienta como parte de un proceso interno de auditoría, se decidió lanzar un scanning sobre la red de la politécnica ingresado un rango de direcciones IP.

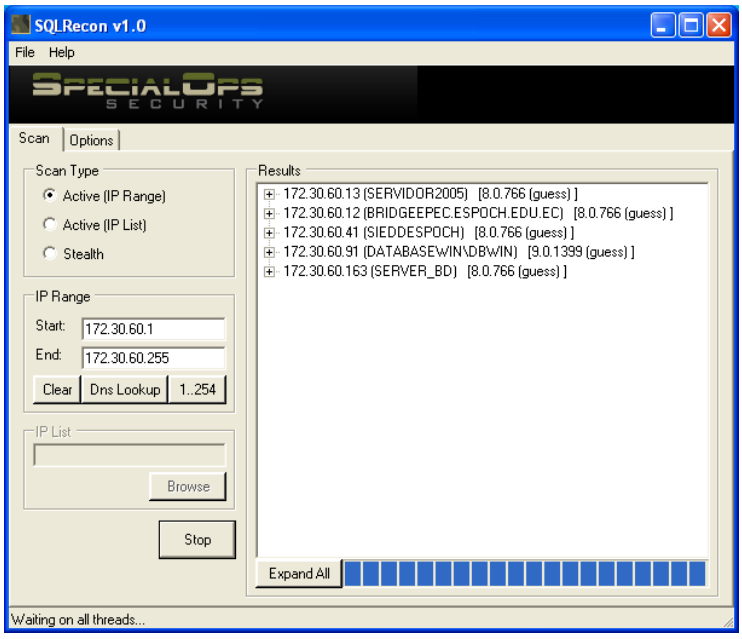


Figura IV.37. Pantalla de SQLRecon

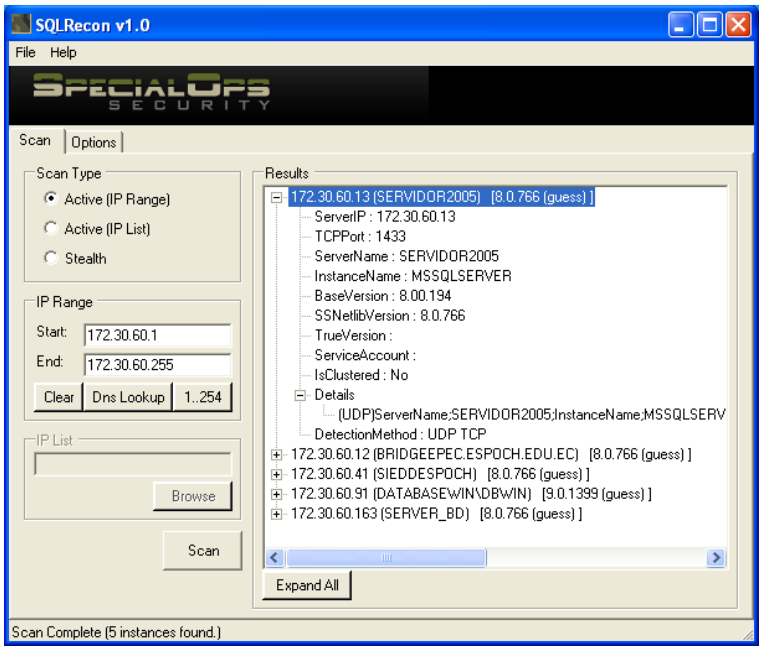


Figura IV.38. Escaneo con SQLRecon

En esta ventana se puede observar la dirección IP del servidor de SQL Server 2005 y el puerto que está usando.

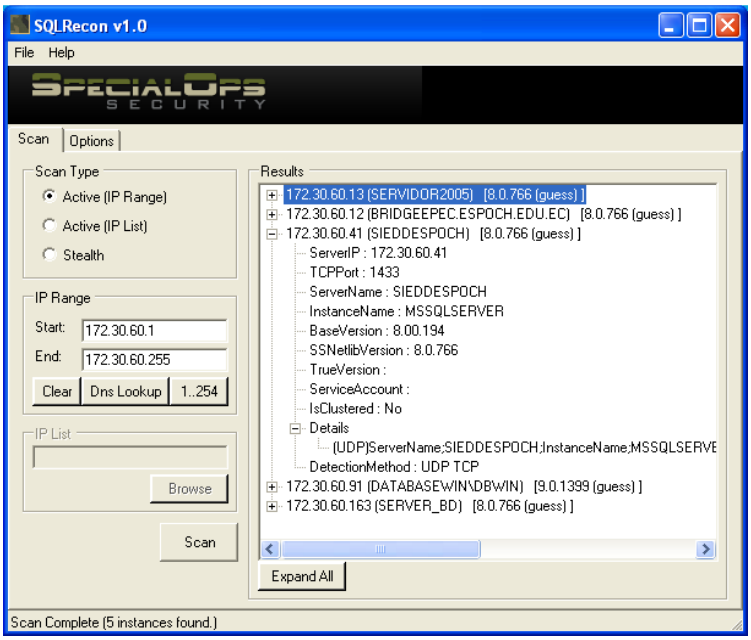


Figura IV.39. Información del escaneo con SQLRecon

WEBCRUISER

Definición

Es una compacta pero potente herramienta de escaneo de seguridad web que le ayudará en las auditorías de su sitio web. Posee un escáner de vulnerabilidades y una serie de herramientas de seguridad. Puede soportar escaneo de sitios web además de POC (prueba de conceptos) para vulnerabilidades web: inyección SQL, Scripting de sitios cruzados, inyección XPath, etc. Por lo tanto, WebCruiser es además una herramienta automática de inyección SQL, herramienta de inyección XPath, y una herramienta de scripting de sitios cruzados.

Características:

- Escáner de vulnerabilidad (inyección SQL, scripting de sitios cruzados, inyección XPath).
- POC (prueba de conceptos): (inyección SQL, scripting de sitios cruzados, inyección XPath).
- Inyección GET/Post/cookie.
- Servidor SQL: Inyección de texto plano/union/ciego.
- MySQL: Inyección de texto plano/union/ciego.
- Oracle: Inyección de texto plano/union/ciego/scripting de sitios cruzados...
- DB2: inyección union/ciega.
- Access: inyección union/ciega.
- Búsqueda de entrada de administración.
- Retrasos de tiempo para búsqueda de inyección.
- Elaborar informe de salidas.

Utilidad

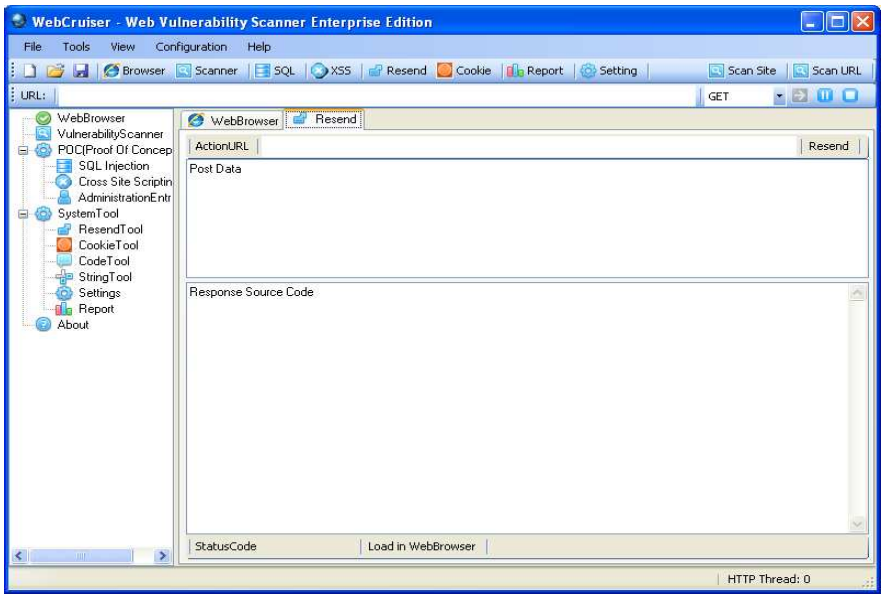


Figura IV.40. Pantalla de WebCruiser

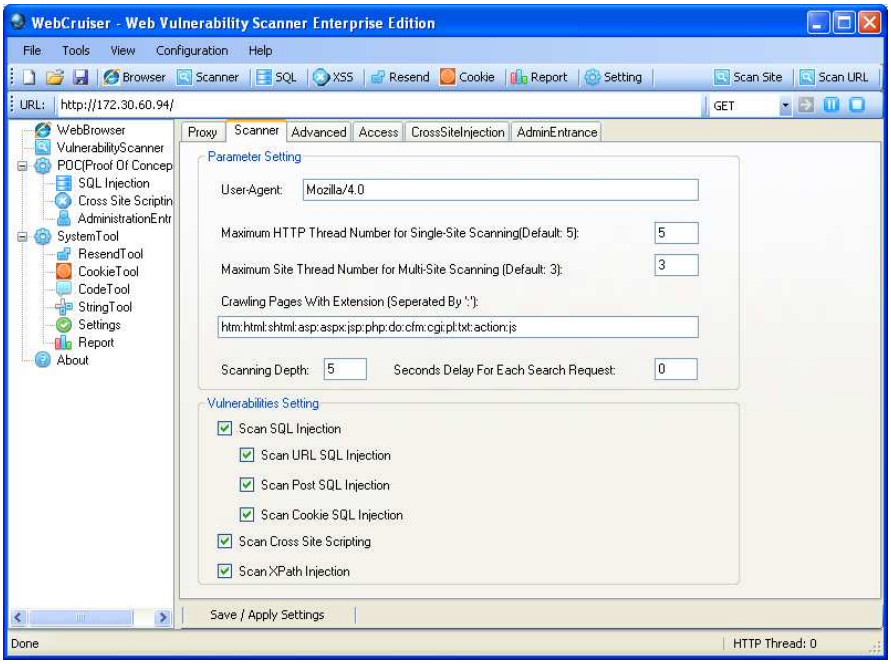


Figura IV.41. Pestaña de Configuración de scanner WebCruiser

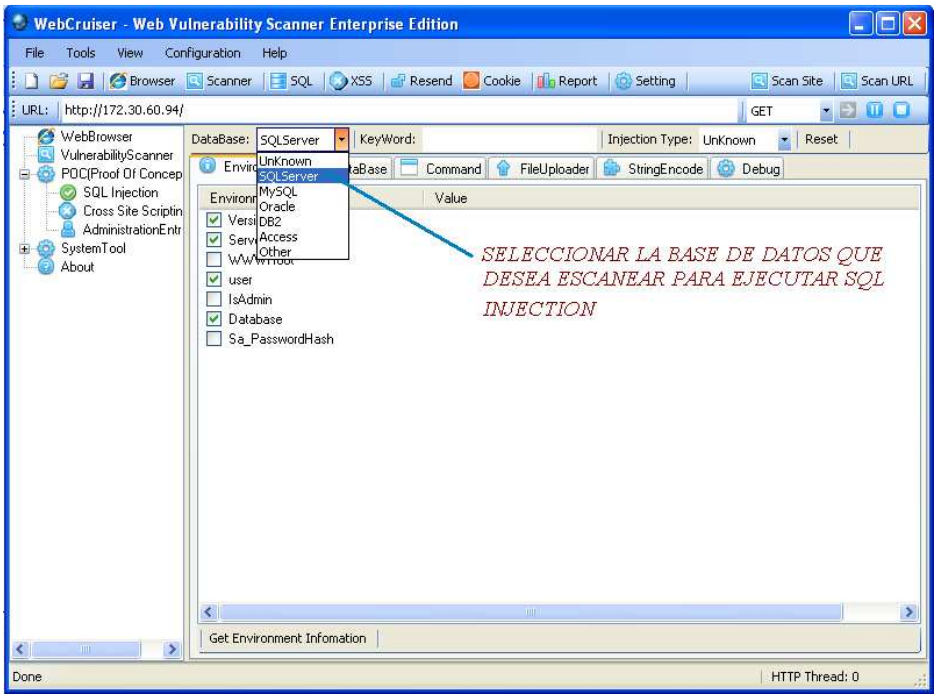


Figura IV.42. Seleccionar la base de datos a escanear

Tabla IV.VIII Cuadro resumen de herramientas software de vulnerabilidad en BD

HERRAMIENTA	PRECIO	REQUERIMIENTOS	DBMS
ACUNETIX WEB VULNERABILITY SCANNER	$1445.00	**Sistemas Operativos Compatibles:** Windows NT/XP/2003/Vista **Requisitos HW** - 256 MB de RAM mínima y recomendadada 512Mb+ - Espacio disponible en disco: 80 GB o mas - Procesador Pentium III o Athlon 1GHz	Microsoft SQL Server
HAVIJ	Libre	**Sistemas Operativos Compatibles:** Windows NT/XP/2003/Vista **Requisitos HW** - 256 MB de RAM mínima y recomendable 512Mb+ - Espacio disponible en disco: 8 MB o mas - Procesador Pentium III o Athlon 1GHz	MySQL Microsoft SQL Server
NGSSQUIRREL	Pagada	**Sistemas Operativos Compatibles:** Windows NT/XP/2000/Vista **Requisitos HW** - 256 MB de RAM mínima y recomendable 512Mb+ - Espacio disponible en disco: 8 MB o mas - Procesador Pentium III o Athlon 1GHz	Microsoft SQL Server
N-STALKER	$1400 - $6300	**Sistema Operativo Compatibles:** Win2000/NT/XP/ 2003 o Vista. **Requisitos HW** - 128 MB de RAM mínima y recomendable 512 MB - Espacio disponible en disco: 500 MB o mas - Procesador mínimo 1GHz y recomendable 2GHz o superior	Microsoft SQL Server
SQL RECON	Pagada	**Sistema Operativo Compatibles** Microsoft Windows 2000, XP, 2003 .NET Framework v1.1 (non-packaged version only) **Requisitos HW** - 512 MB de RAM mínima y recomendable 1GB - Espacio disponible en disco: 80MB o mas - Procesador Pentium III o superior	Microsoft SQL Server
WEB CRUISER	$ 49.00	**Sistema Operativo Compatibles** Windows XP/Vista/7 (32/64 bit) .NET Framework v1.1 (non-packaged version only) **Requisitos HW** - 512 MB de RAM mínima y recomendable 1 GB - Espacio disponible en disco: 80MB o mas - Procesador Pentium4 o superior	MySQL Microsoft SQL Server

4.3. HERRAMIENTAS DE REPARACIÓN Y RECUPERACIÓN DE BASES DE DATOS

Existen herramientas diseñadas para reparar y recuperar los archivos dañados de base de datos a causa de un ataque de virus, apagado inesperado del sistema, error de lectura de los medios de comunicación y así sucesivamente. Para la recuperación de la base de datos se puede utilizar Software que permite recuperar todos los componentes de la base de datos incluyendo tablas, claves primarias y las relaciones.

RECOVERY FOR MYSQL

Definición

Es un software de recuperación de datos de gran alcance para los archivos dañados de bases de datos MySQL Server (. MYD y. MYI). En caso de fallo repentino de base de datos, la recuperación fiable de los datos esenciales de emergencia a menudo es de vida o muerte. Recuperación para MySQL cumple perfectamente con estos requisitos. Guarda la información recuperada en el ajuste de secuencia de comandos Transact-SQL para la recreación de base de datos rápida. Recupera la estructura de tabla y los datos, los índices de recuperación de datos. Fácil de usar, no se requieren habilidades especiales.

Características

Recupera archivos de bases de datos MySQL (. MYD,. MYI) y guarda los datos recuperados en una secuencia de comandos SQL

- Restaura la estructura de la tabla y los datos
- Recupera los índices
- Fácil de usar, no se requieren habilidades especiales
- Completa de install / uninstall

Utilidad

Recovery for MySQL permite recuperar la base de datos al dar click en Recover, al dar click en esta opción el programa permitirá mostrar una pantalla en donde hay que seleccionar la base de datos a recuperar.

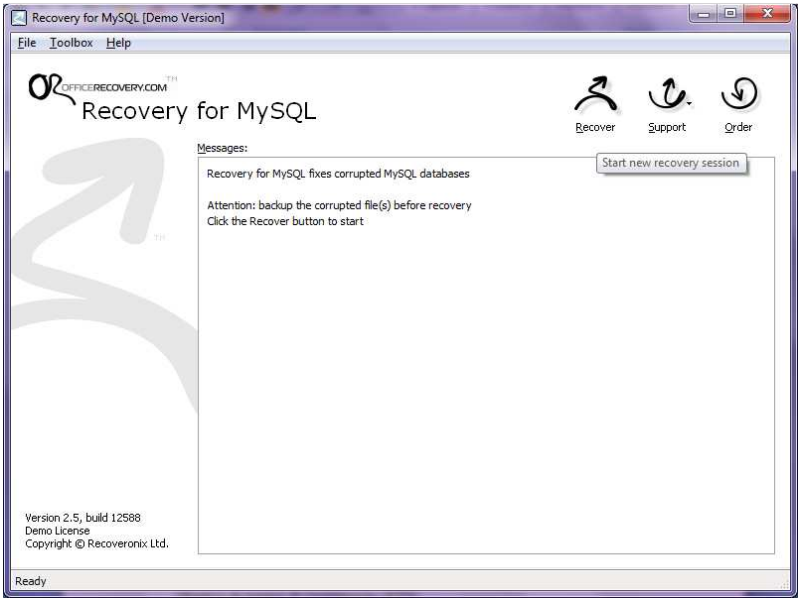


Figura IV.43. Pantalla principal Recovery for MySQL

Una vez seleccionada la base de datos, escoger la carpeta destino en la cual se va a recuperar la información, para terminar con la recuperación dar clic en start.

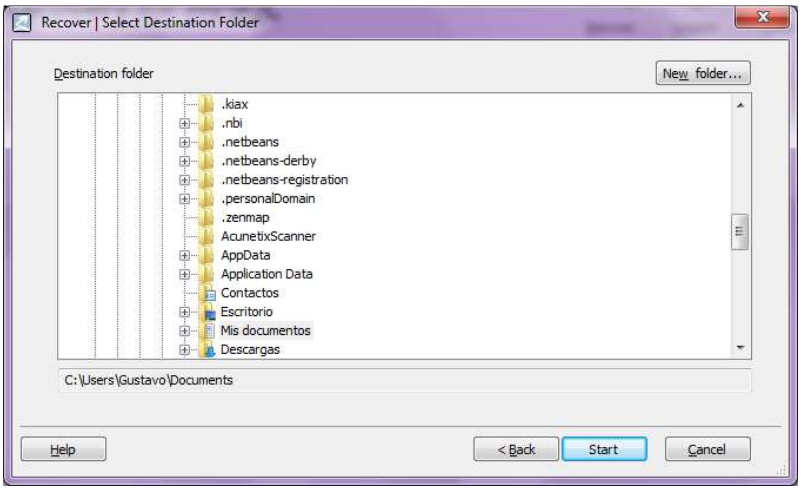


Figura IV.44. Carpeta destino para recuperación

ACRONIS RECOVERY FOR MS SQL SERVER

Definición

Acronis Recovery for MS SQL Server proporciona una tecnología probada de copia de seguridad de bases de datos que reducirá drásticamente el tiempo de recuperación después de una catástrofe, para que pueda volver a trabajar en cuestión de minutos en vez de horas. La Recuperación en un paso y la Recuperación automática al punto de error reducen el tiempo de desconexión y ayudan a su organización a mejorar su Objetivo de tiempo de recuperación (RTO).

Características

- Realice la copia de seguridad y restauración de bases de datos o de instancias enteras
- Recuperación automática al punto de error
- Ajuste la estrategia de copias de seguridad con un asistente
- Cree un plan de recuperación de catástrofes

Utilidad

Una vez instalado el programa se presenta la pantalla de inicio en donde seleccionar la opción **Conectar a un equipo remoto** si se conoce el equipo caso contrario elegir **Buscar servidores**

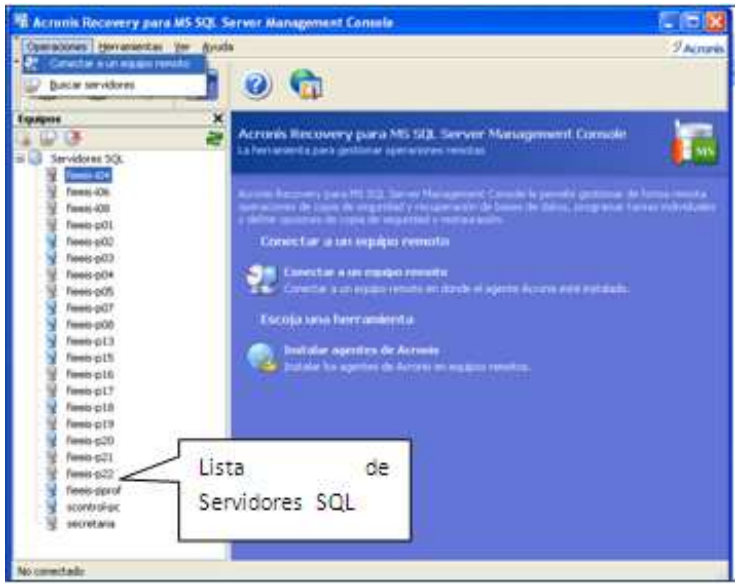


Figura IV.45. Lista de Servidores SQL

Buscar servidores permite encontrar todos los servidores que se encuentran en la red, de esta forma elegimos el servidor que deseamos.

Una vez seleccionado el servidor proceder a conectar con el equipo

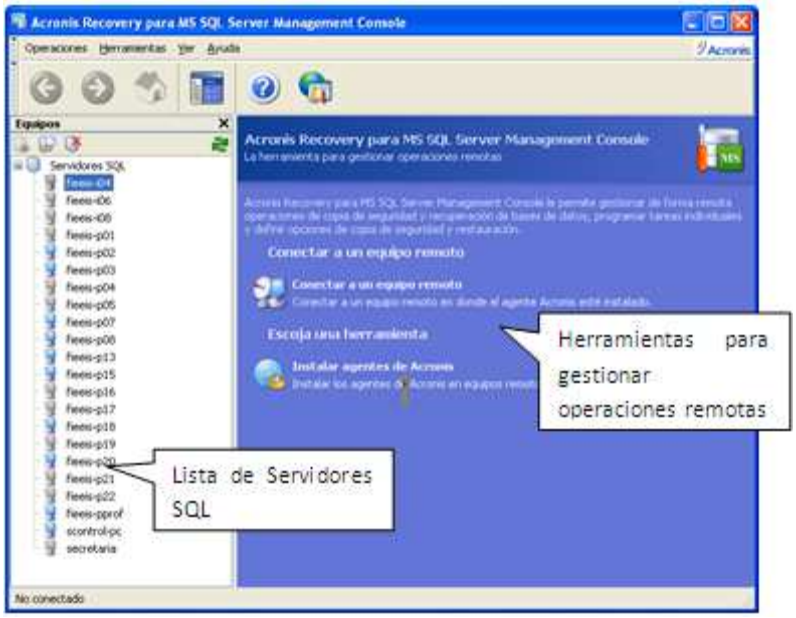


Figura IV.46. Herramientas para gestionar operaciones remotas

La herramienta muestra el tiempo que demora del proceso.

Figura IV.47. Recuadro procesando

Una vez ingresado al servidor el programa permite escoger algunas opciones como: Copia de seguridad, Restaurar, Limpieza de la ubicación de la copia de seguridad, Plan de recuperación de desastres, etc. Lista de Tareas para SQL Server en: FIEEIS-I03

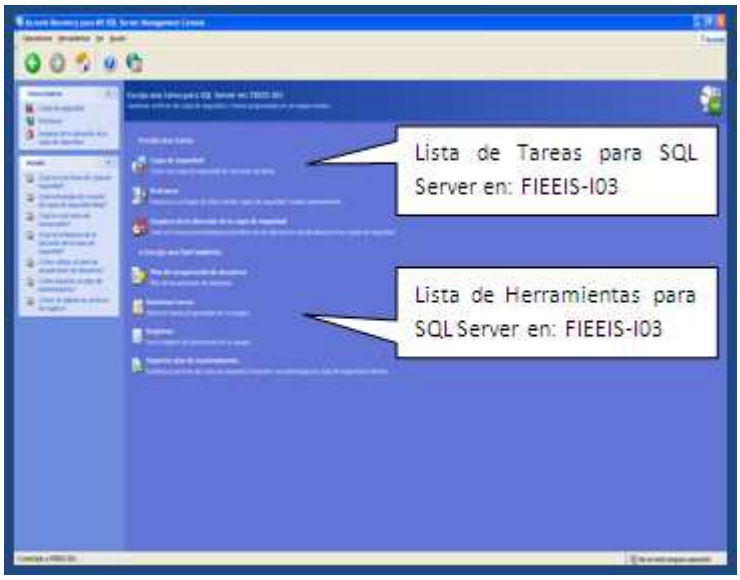


Figura IV.48. Lista de tareas y herramientas

Al elegir copia de seguridad se visualizara una pantalla en donde se debe definir la estrategia de la copia de seguridad de acuerdo a nuestras necesidades.

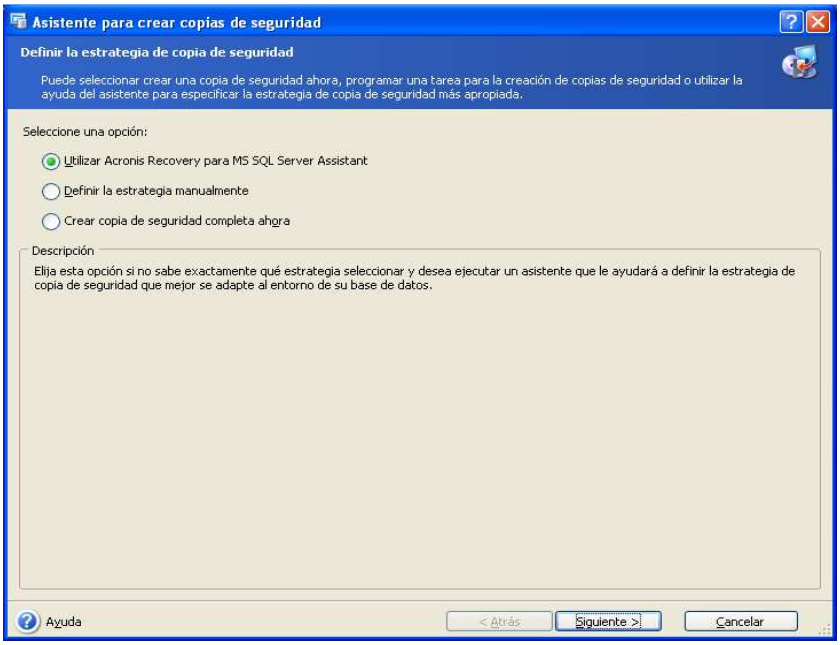


Figura IV.49. Asistente para crear copias de seguridad

Luego ingresar el nombre del usuario y la clave esta opción se presenta si se escoge la opción Utilizar Acronis Recovery para MS SQL Server Assistant

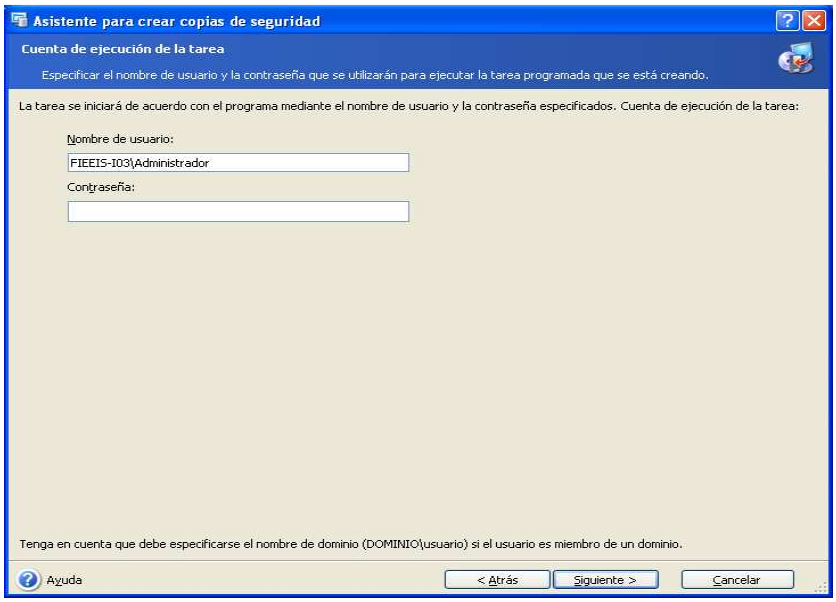


Figura IV.50. Cuenta de ejecución de la tarea

Pero al elegir la opción Crear copia de seguridad completa ahora los pasos a seguir serán los siguientes:

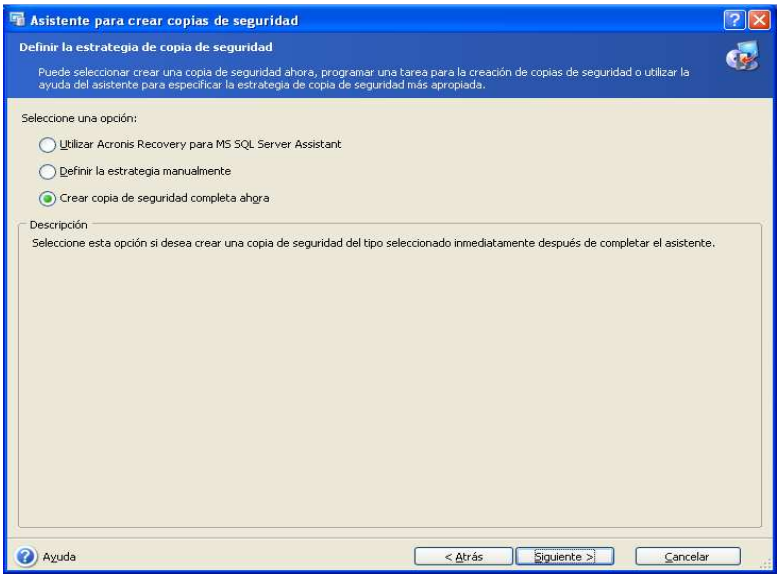


Figura IV.51. Estrategias de copia de seguridad

Primero elegir los objetos que se desea incluir en la copia de seguridad

Luego seleccionar la ubicación de la carpeta de seguridad.

Figura IV.52. Ubicación de la copia de seguridad

A continuación, seleccionar la opción Utilizar las opciones predeterminadas o configurar las opciones manualmente

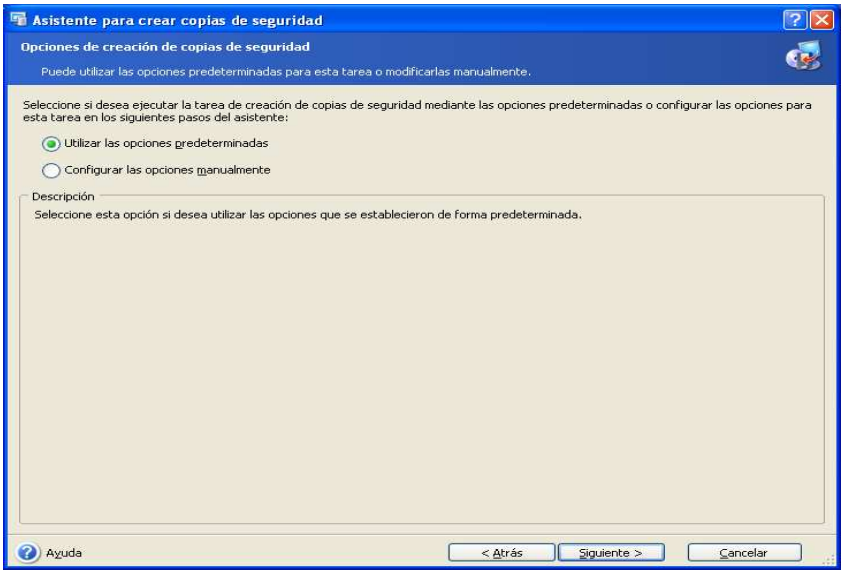


Figura IV.53. Operaciones de creación de copia de seguridad

Luego ingresar el nombre de la tarea, dar clic en siguiente.

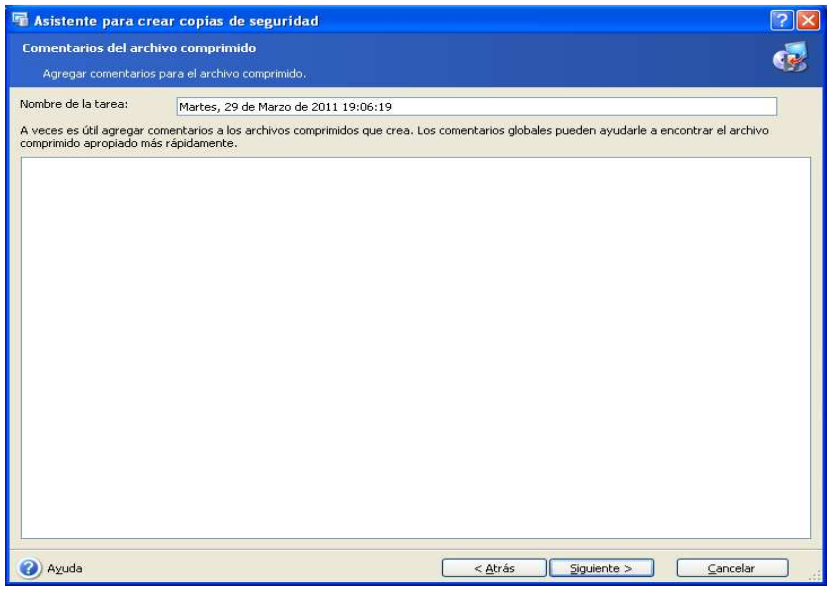


Figura IV.54. Comentarios del archivo comprimido

Y finalmente se visualiza una lista completa de las operaciones que se realizara, dar clic en finalizar para terminar con la realización de la copia de seguridad

Figura IV.55. Lista de operaciones a realizarse

Si la operación es correcta el programa indicara si se ejecuto correctamente o si ocurrió algún error.

Restaurar permite recuperar la base de datos de acuerdo a dos opciones

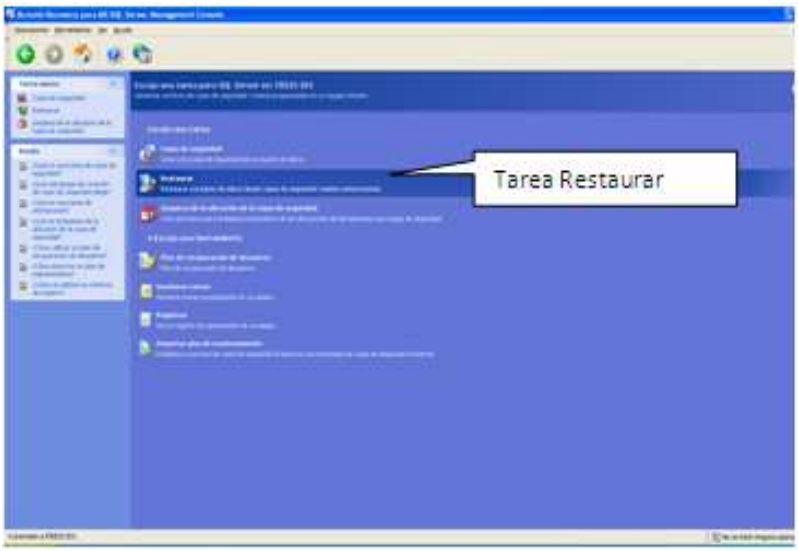


Figura IV.56. Tarea Restaurar

Las opciones de restauración son: Ahora y según programado esta opción permite restaurar de acuerdo a fechas en las que se hicieron las copias de seguridad

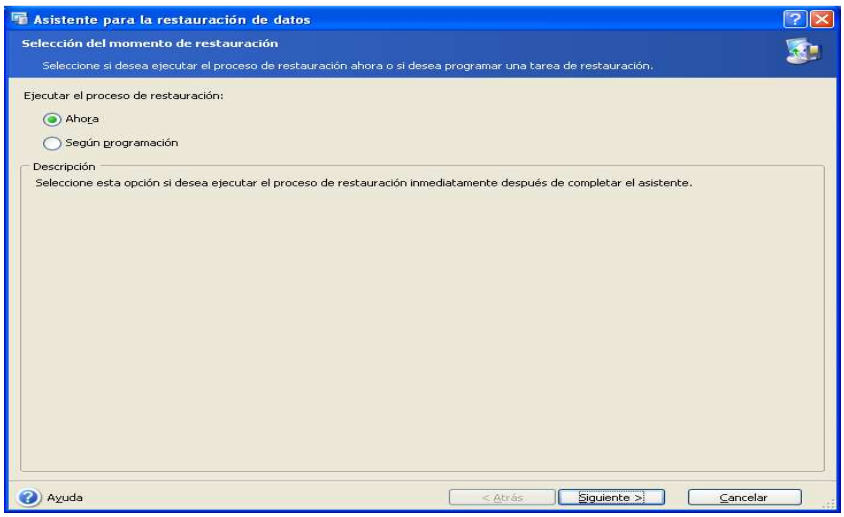


Figura IV.57. Asistente para la Restauración de Datos

Al elegir la primera opción primero seleccionar la carpeta en donde está la copia de seguridad

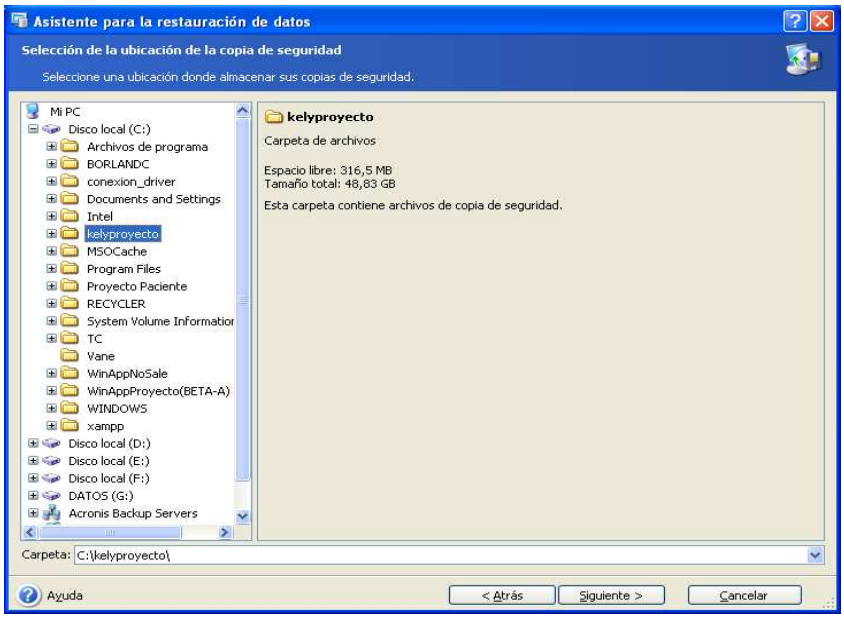


Figura IV.58. Ubicación de la Copia de Seguridad

Luego seleccionar el punto de restauración, en este caso elegir **Restaurar al punto de fallo.**

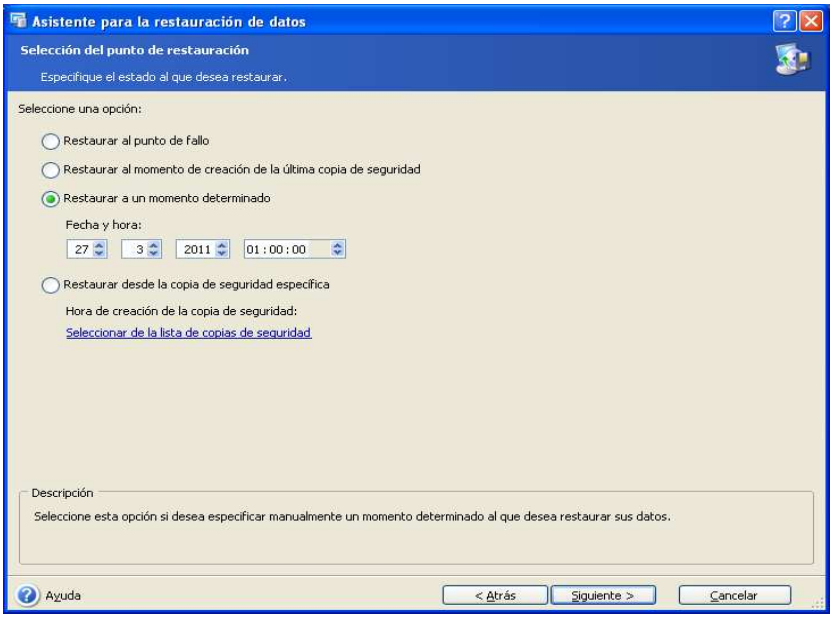


Figura IV.59. Selección del punto de restauración.

Seguidamente seleccionar la base de datos que se va a restaurar.

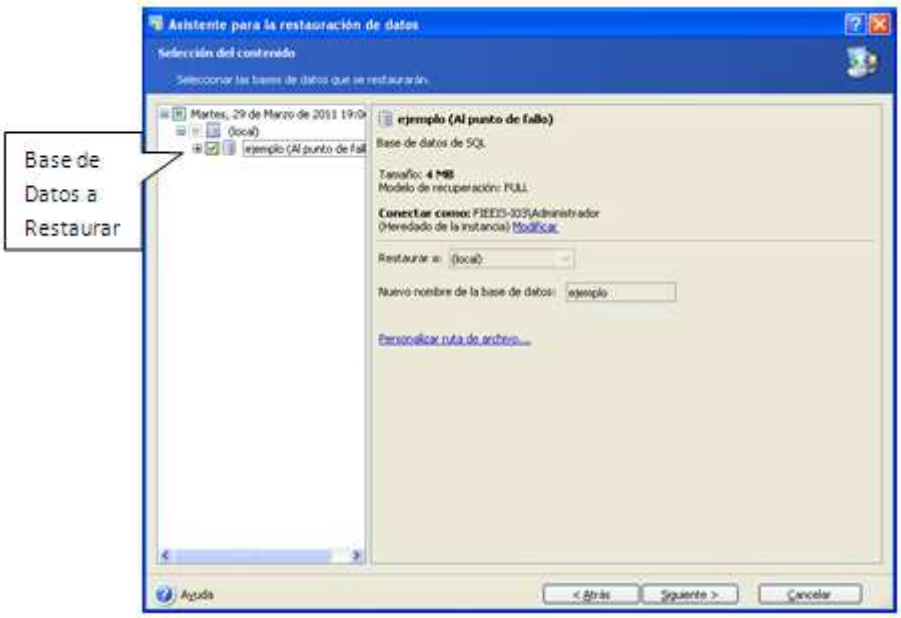


Figura IV.60. Selección de la base de datos que se restaurara.

Seleccionar las opciones de restauración, dar click en siguiente.

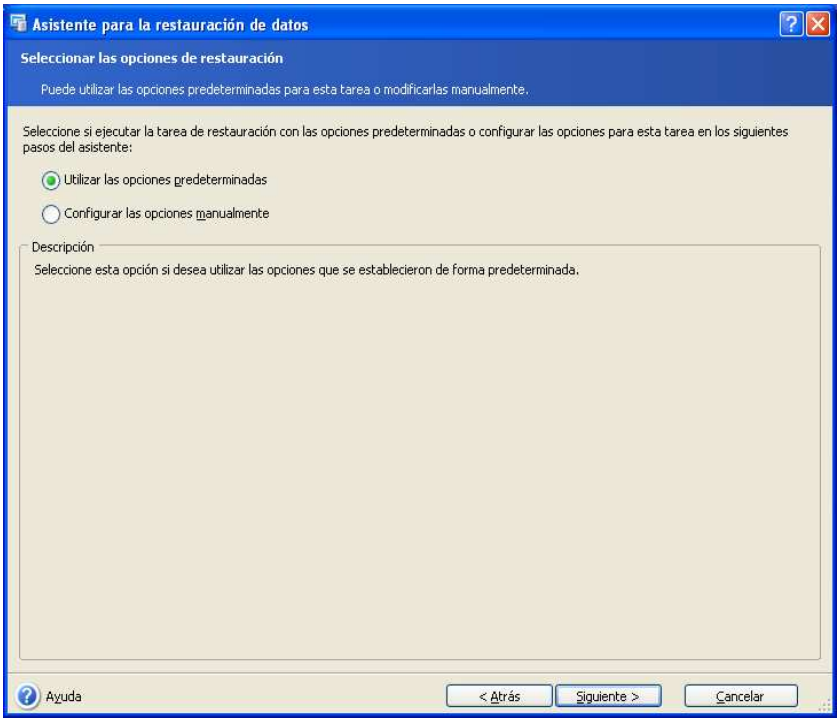


Figura IV.61. Opciones de restauración.

La herramienta muestra una lista completa de todas las operaciones que se va ha realizar, dar clic en finalizar.

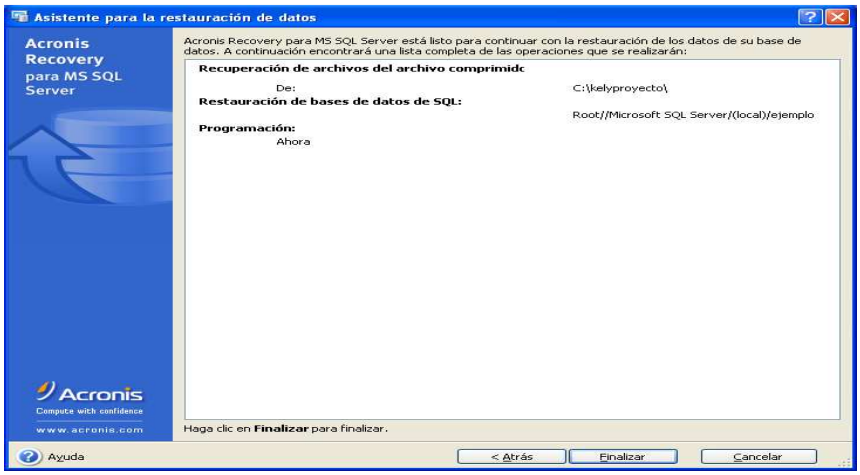


Figura IV.62. Lista completa de operaciones ejecutadas.

Si la operación es exitosa o tiene errores el programa mostrará estas opciones

Si se elige **Plan de recuperación de desastres** la herramienta permitirá gestionar un plan mediante la utilización de un asistente.

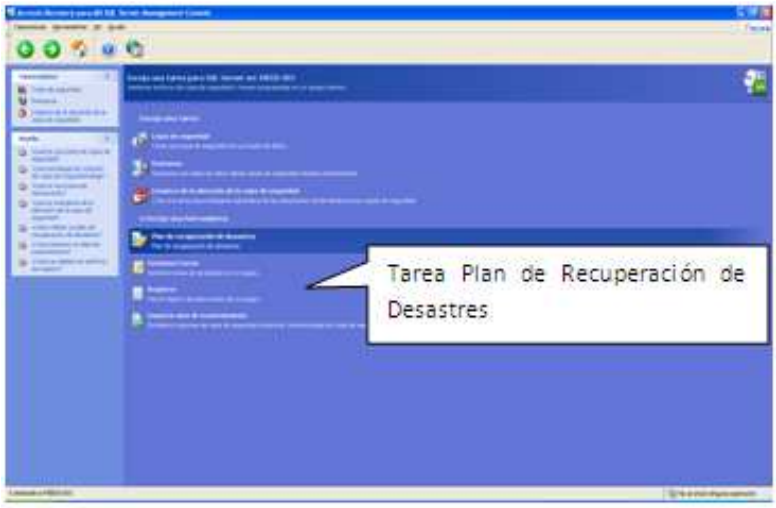


Figura IV.63. Tarea plan de recuperación de desastres.

La herramienta presenta la pantalla del asistente para realizar el plan de recuperación desastres en la cual se debe elegir la base de datos para obtener el plan.

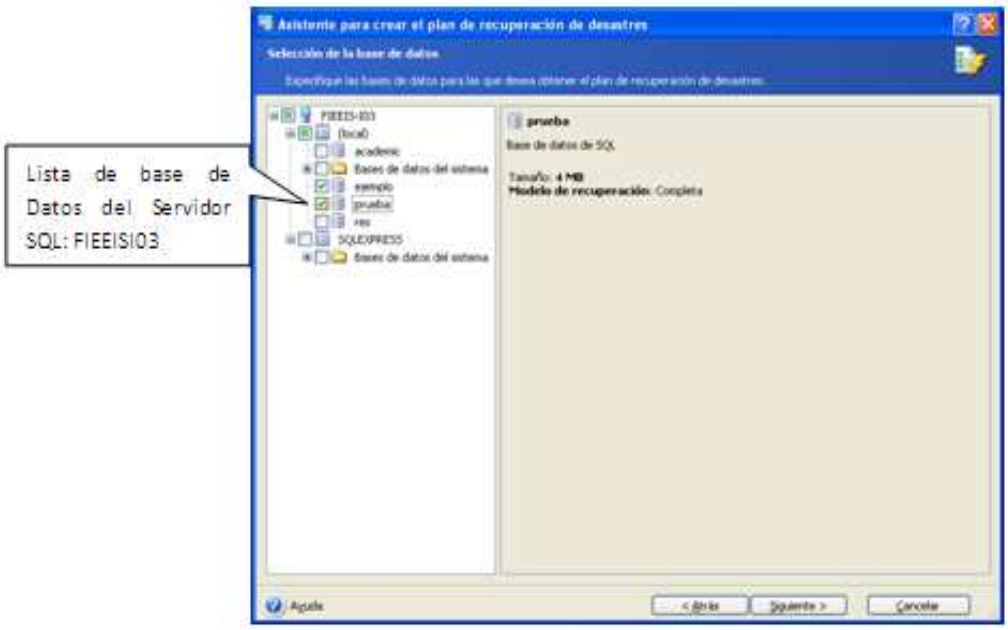


Figura IV.64. Selección de la base de datos

Seleccionar la base de datos ahora elegir el método de envió en mismo que puede ser por medio de correo electrónico o mostrándolo en formato html.

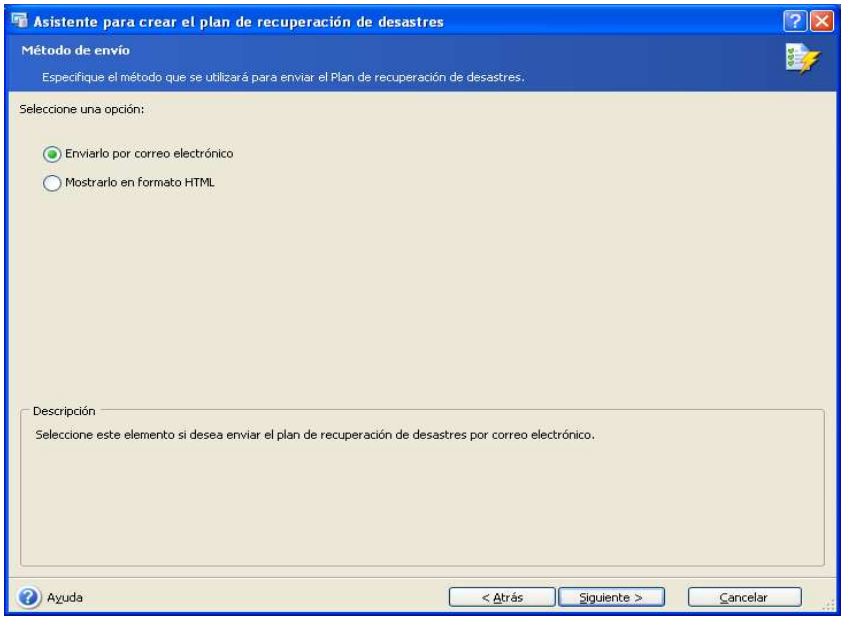


Figura IV.65. Método de envió.

Al seleccionar enviarlo por correo electrónico, el asistente presentara los parámetros del correo electrónico para enviar el plan de recuperación de desastres.

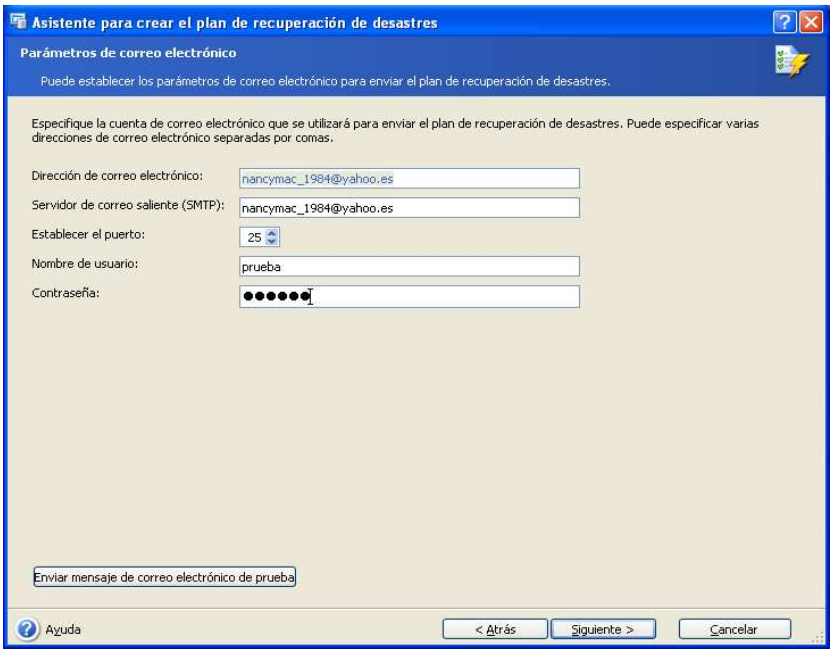


Figura IV.66. Parámetros de correo electrónico.

Una vez especificados los parámetros el asistente presentara una lista completa de ;las operaciones que se van a realizar y por ultimo dar click en finalizar.

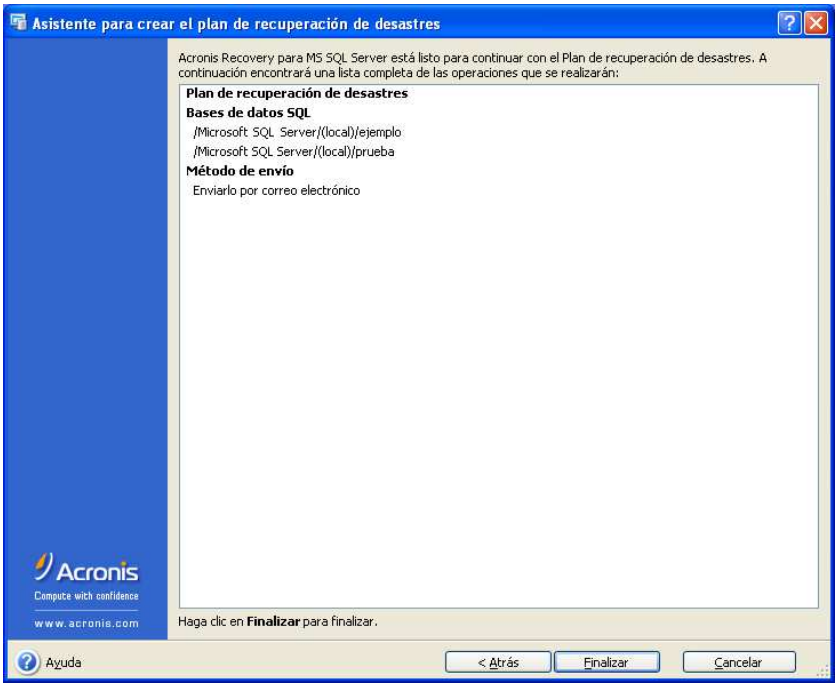


Figura IV.67. Lista completa de las operaciones que se realizaran.

Al dar click en visor de registros el programa permite verificar el estado de las operaciones ejecutadas por Acronis para MS SQL Server.

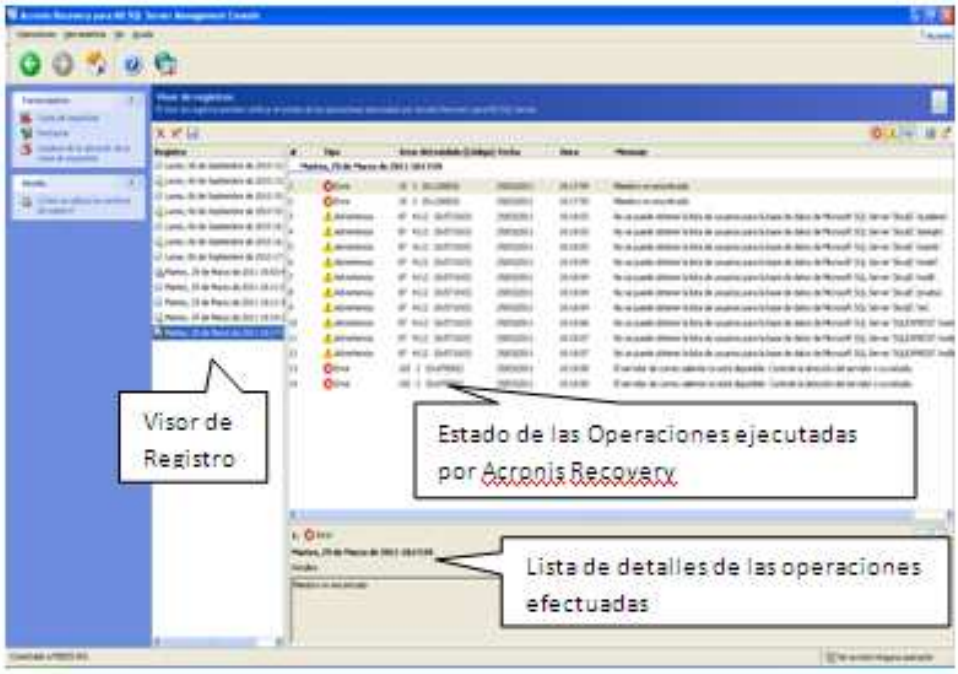


Figura IV.68. Plan de recuperación de desastres.

STELLAR PHOENIX DATABASE RECOVERY FOR MYSQL

Definición

Este software está diseñado para reparar y recuperar los archivos de base de datos corruptos (MYD y. MYI). Las restauraciones de reparación MySQL aplicación dañada. MYD y archivos. MYI por ejemplo, de un ataque de virus, cierre inesperado del sistema, error de lectura de los medios de comunicación y así sucesivamente. El Software de recuperación de Base de datos para MySQL ayuda en la recuperación de todos los componentes de base de datos MySQL Server, incluyendo tablas, claves primarias y las relaciones. Stellar Phoenix Recuperación de la base de datos MySQL utiliza algoritmos de gran alcance, que lleva a cabo completa y exhaustiva exploración del archivo de MySQL con el fin de recuperar la mayor cantidad de datos posible. El software nunca borra o modifica los datos originales, e incluso archivos muy dañados pueden ser óptimamente reparados y restaurados. Sistema de servidor MySQL también

soporta la recuperación de bases de datos MySQL Creación de plataforma Linux o Windows y proporciona una interfaz interactiva, que le hace fácil de usar y fácil de entender.

Características

- Compatible con motores de base de datos MySQL de almacenamiento - MyISAM e InnoDB
- Compatible con InnoDB (. Ibdata. Ibd y. Frm) y MyISAM (. MYD. MYI y. Frm) archivos
- Tiene una interfaz de usuario auto-explicativa para hacer la recuperación de base de datos segura y fácil
- Establece una conexión segura con el servidor MySQL, mientras que la reparación de base de datos dañada (s)
- Recupera datos de tablas en las que se aplican por defecto y las propiedades de incremento automático
- Restaura todos los tipos de datos excepto los tipos de datos espaciales
- Manual de la recuperación de los datos guardados en un único directorio en la ubicación predeterminada de instalación de MySQL
- Permite la recuperación selectiva de los componentes de base de datos MySQL
- No requiere instalación de MySQL a los objetos un fragmento recuperable de corrupción de bases de datos MySQL (s)
- Crea un archivo de registro para guardar los detalles de recuperación que se puede ver en un editor de texto
- Soporta la recuperación de la base de datos MySQL Creación de plataformas Linux y Windows

Utilidad

Para iniciar la herramienta Stellar Phoenix Recuperación de bases de datos para MySQL se sigue los siguientes pasos:

1. Haga clic en Inicio | Programas | Stellar Phoenix Recuperación de bases de datos para MySQL y seleccione Stellar Phoenix MySQL Recovery para abrir la herramienta. El Stellar Phoenix Recuperación de bases de datos MySQL para la ventana se abre:

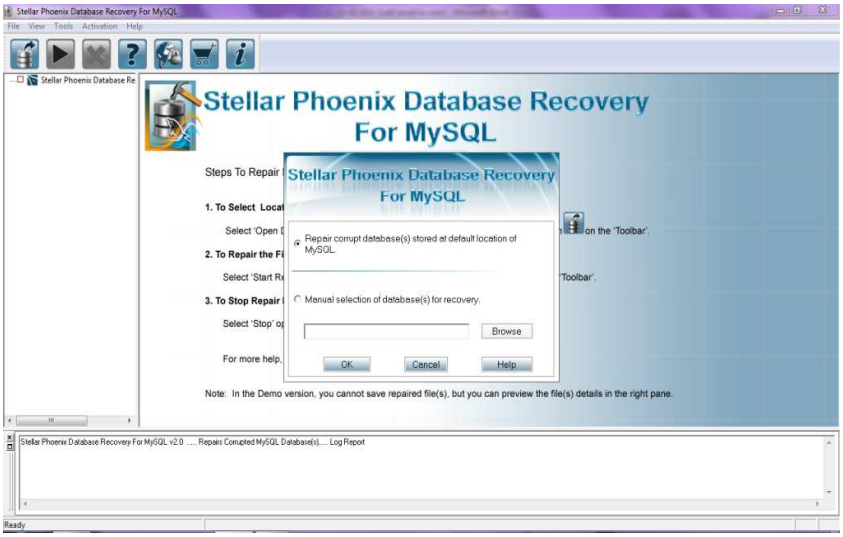


Figura IV.69. Pantalla principal de Stellar Phoenix MySQL Recovery

La ventana principal de este software está compuesta por tres paneles. El panel izquierdo muestra la estructura de árbol de la base de datos (s). El panel derecho muestra los detalles de la base de datos (s) de archivos. El panel inferior nombrado como Messagelog muestra la transformación de un proceso continuo.

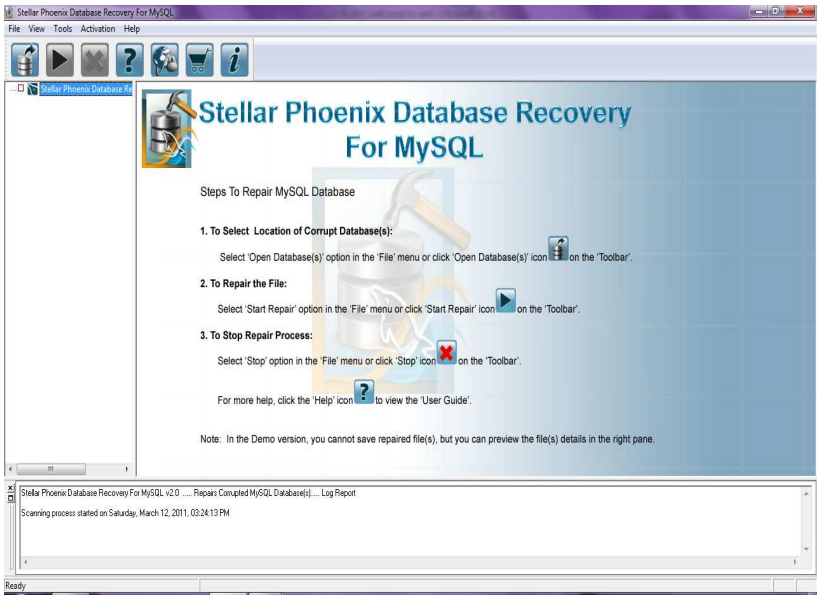


Figura IV.70. Paneles principales de Stellar Phoenix MySQL Recovery

SYSTOOLS SQL RECOVERY

Definición

SysTools SQL Recovery es un programa para la recuperación las bases de datos SQL, permite reparar las bases de datos corruptas en SQL, cuenta con herramientas para la recuperación de los datos, tablas, vistas, disparadores, procedimientos almacenados, reglas por defecto, tipos de datos definidos por el usuario y los factores desencadenantes de las bases de datos MDF corruptas. SysTools SQL Recovery es compatible con Microsoft SQL Server 2000.

Características

- Herramienta de recuperación de MDF para recuperar tablas, procedimientos almacenados, vistas, índices, etc
- Recupera valores por defecto y predefinidos, las reglas, limitar los "cheques", tipos de datos de usuario, etc
- Recupera archivos MDF, claves principales, clave única, claves externas de archivos corruptos de MDF.
- Recupera disparadores, procedimientos almacenados y recupera la base de datos SQL de forma instantánea
- Importa información recuperada en una bases de datos SQL Server o en un saperate archivo de secuencia de comandos SQL.
- Fácil proceso de base de datos corruptos de Microsoft SQL (Servidor de Base de Datos), archivo MDF y crea un script SQL con la estructura de base de datos recuperada y los datos

Utilidad

Para iniciar esta herramienta primero seleccionar la ruta del archivo .mdf.

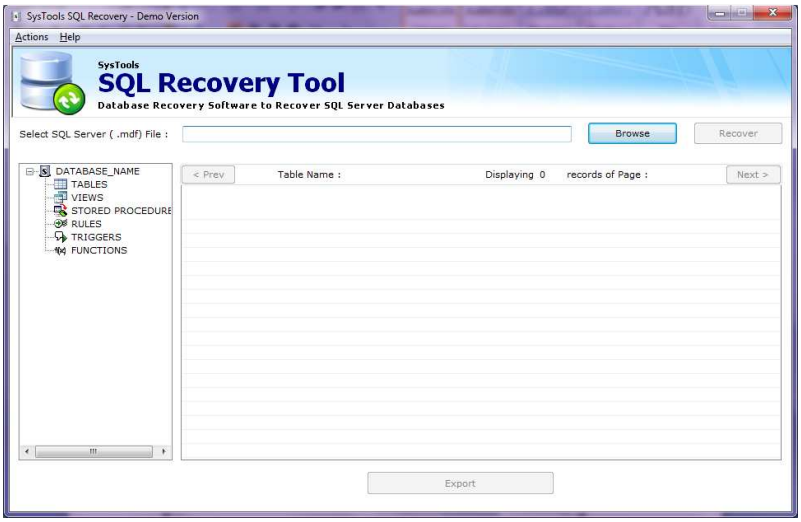


Figura IV.71. Ventana principal de SQL Recovery Tool

Seleccionar el archivo a recuperar y damos click en abrir.

Una vez seleccionado el programa muestra el porcentaje de carga del proceso y se visualizara una lista detallada del contenido del archivo mdf.

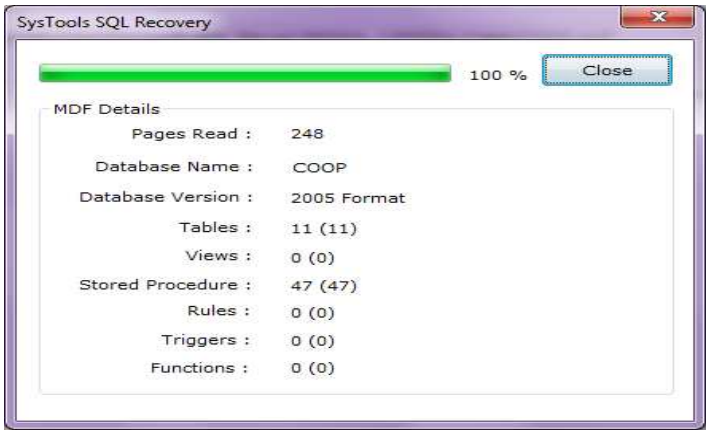


Figura IV.72 Porcentaje de carga del proceso

Al terminar el proceso se muestra la siguiente pantalla en donde se visualiza el contenido de la base de datos a recuperar.

Figura IV.73 Lista de datos recuperados

Como se puede observar esta herramienta nos muestra las tablas, procedimientos almacenados, vistas, claves, etc.

Figura IV.74 Descripción de la estructura de la base de datos

La herramienta recupera también el contenido de las tablas como se puede observar en la siguiente pantalla.

Figura IV.75 Descripción de los datos de las tablas recuperadas.

De igual manera se podrá ver la información de los procedimientos almacenados.

Figura IV.76 Lista de procedimientos almacenados.

Una vez seleccionada la información a recuperar dar click en Export el cual permite guardar y recuperar la base de datos al dar click en esta opción la herramienta pedirá que se ingrese el tipo de **Export** , llenar las credenciales de la base de datos y finalmente dar click en **Export/Save.**

Figura IV.77. Información recuperada

STELLAR PHOENIX SQL RECOVERY

Definición

Este MS SQL Server es un software de recuperación muy fácil de utilizar utilidad que repara y recupera dañados bases de datos SQL sin ninguna modificación

Características

- Recupera tablas, vistas y las Reglas
- Recuperar de procedimientos almacenados y disparadores
- Recupera valores predeterminados y las limitaciones por defecto
- Funciones definidas por el usuario recupera y definido por el usuario los tipos de datos
- Recuperación de la clave principal, claves externas, claves únicas e Identidad
- La recuperación de índices y restricciones CHECK
- Recuperación de la unión de Incumplimiento y el Reglamento con las columnas de la tabla definida por el usuario y tipos de datos.

- La recuperación de. Ndf base de datos de archivos

Utilidad

La herramienta presenta una amplia gama de opciones para la recuperación de base de datos

Figura IV.78. Elección del archivo a recuperar.

Antes de elegir el archivo a recuperar se debe parar el servicio de SQL SERVER para que funcione el programa.

Parado el servicio dar click en **Open MS SQL file to be repaired**, al seleccionar esta opción el programa visualizara una ventana en donde se debe elegir la ruta del archivo a recuperar.

Al seleccionar la ubicación del archivo el programa mostrara los resultados de la información del archivo.

El programa mostrara el contenido de la base de datos a recuperar

Figura IV.79. Lista completa de los datos a recuperar.

Se visualiza las tablas, procedimientos, vistas, claves principales, etc

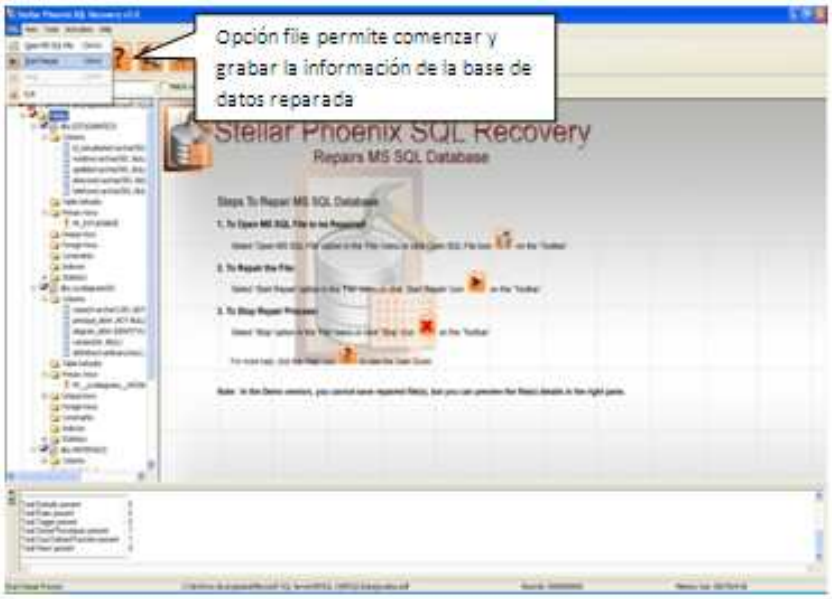


Figura IV.80. Opción file.

Finalmente dar click en **Repair the file** y guardar el archivo recuperado

RECOVERY FOR SQL SERVER

Definición

Recuperación para SQL Server software de recuperación de datos para los corruptos de bases de datos Microsoft ® SQL Server, copias de seguridad y los registros

Características

- Recuperación para SQL Server reparaciones dañado bases de datos SQL Server, copias de seguridad y los registros (. Mdf,. Ndf. Bak,. Ldf).
- Compatible con SQL Server 2008 de archivos cifrados
- Recupera copias de seguridad comprimidas de SQL Server 2008
- Recupera SQL Server 2005, 2008 de datos comprimidos (tipos de filas, RAGE)
- Recupera SQL Server 2008 FILESTREAM tipo de datos. Tenga en cuenta que la base de datos deben ser recuperados en el mismo equipo donde se encuentra la base de datos original
- Recupera varchar (máx.) tipo de datos

Utilidad

Antes de utilizar esta herramienta se debe detener el servicio de SQL, para continuar con la recuperación dar click en **Recover.**

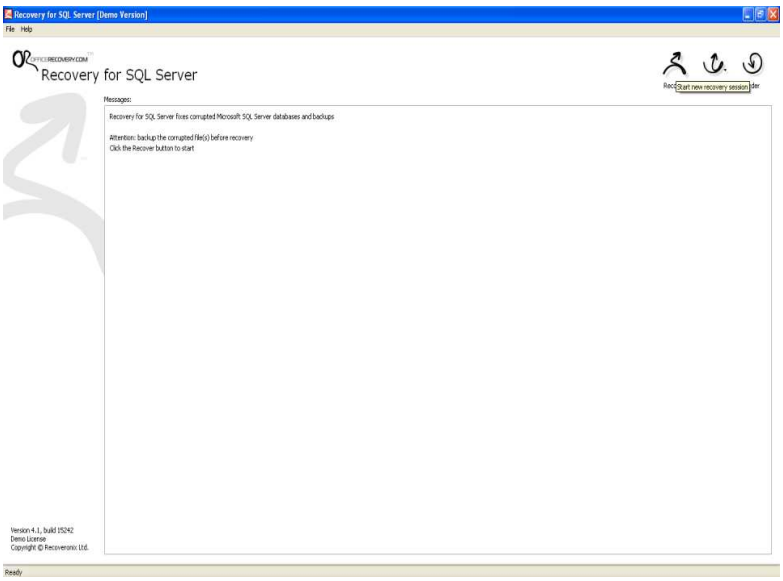


Figura IV.81. Ventana principal de Recovery for SQL Server.

Esta opción permite al usuario localizar el archivo mdf que va ser recuperado. Seleccionar el archivo a recuperar y dar click en **Next.**

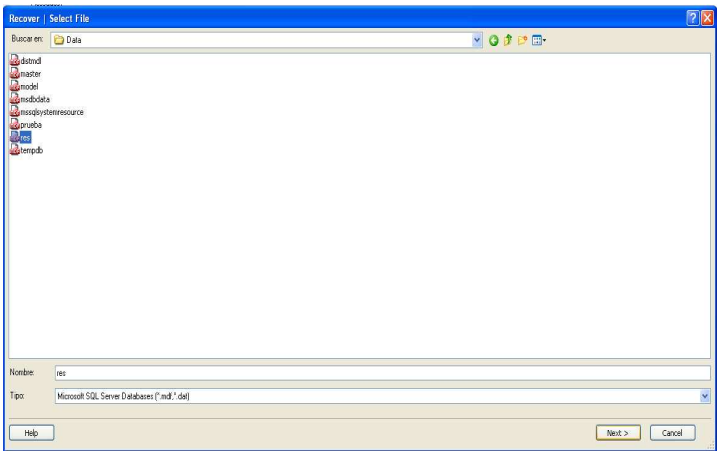


Figura IV.82. Ubicación del archivo .mdf

Si la herramienta es un demo como se *presentara* la siguiente pantalla de aviso sobre la licencia dando una notificación de limitada, caso contrario continuara con la reparación.

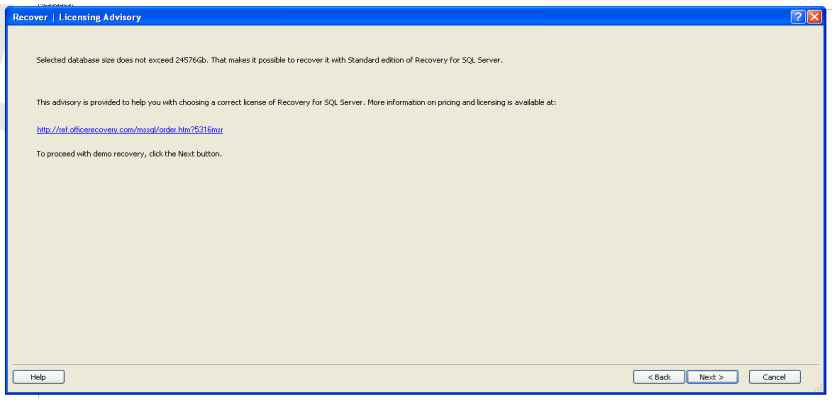


Figura IV.83. Verificación de licencia

La herramienta muestra dos tipos de reparación **Typical y Custom**. La elección de la opción dependerá de las necesidades, elegir la opción y dar click en Next.

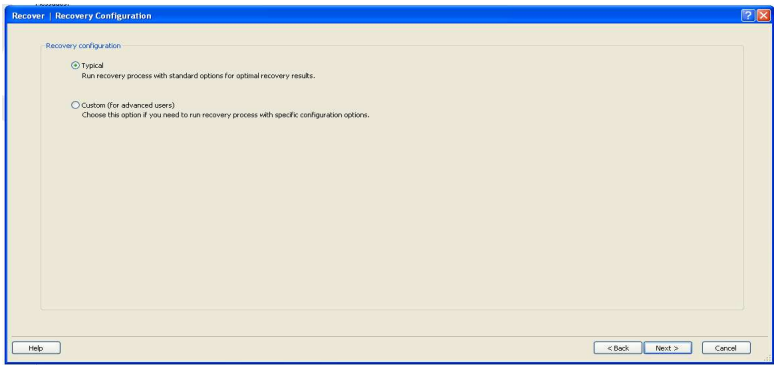


Figura IV.84. Tipos de reparación

Antes de realizar la reparación se debe crear una carpeta en la ubicación que se desea, esta carpeta contendrá toda la información de la base de datos recuperada. Seleccionar la carpeta creada.

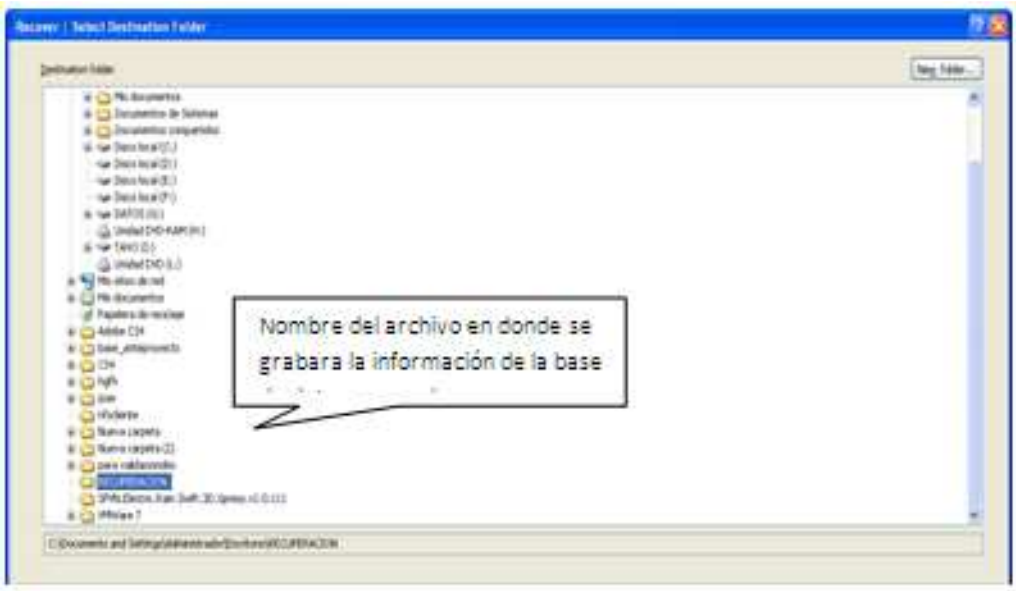


Figura IV.85. Ubicación del archivo donde se guardara la información

Una vez seleccionada la carpeta el programa muestra el porcentaje del proceso de recuperación.

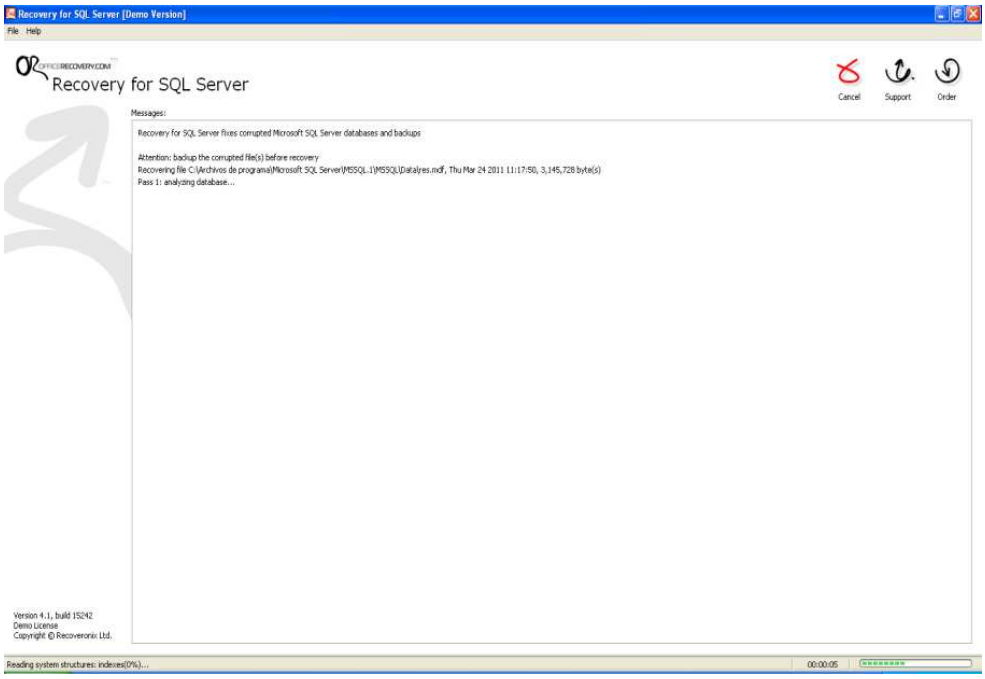


Figura IV.86. Porcentaje del proceso de recuperación

En la siguiente pantalla introducir el nombre del servidor SQL y el tipo de autenticación

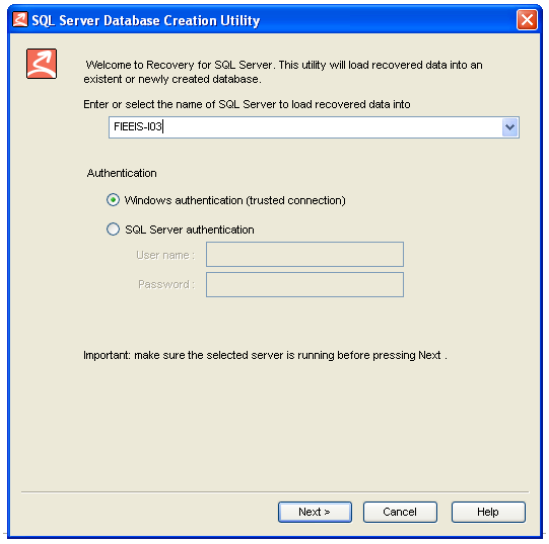


Figura IV.87. Nombre del servidor SQL y el tipo de autenticación

Luego seleccionar el modo correcto para importar nuestra información.

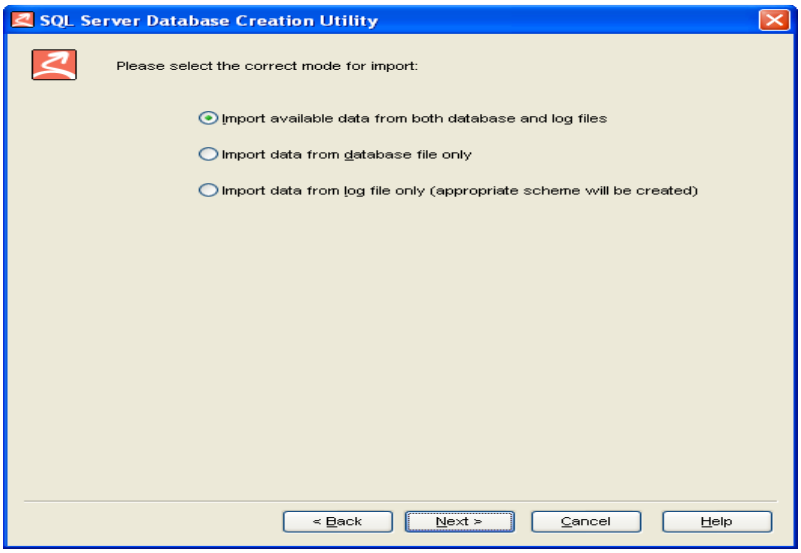


Figura IV.88 Modo para importar.

Seleccionado el modo el programa se mostrara la información a recuperar

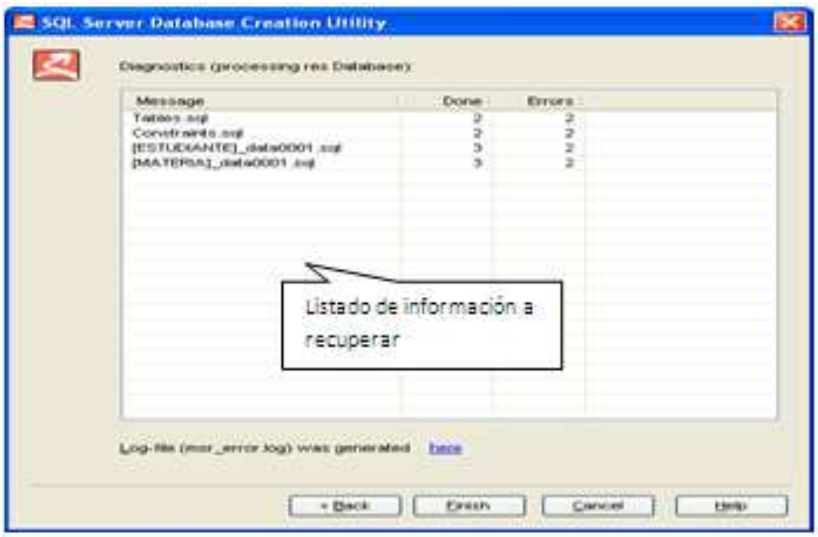


Figura IV.89. Listado de información a recuperar

Una vez finalizada la recuperación proceder a abrir la carpeta creada con este fin.

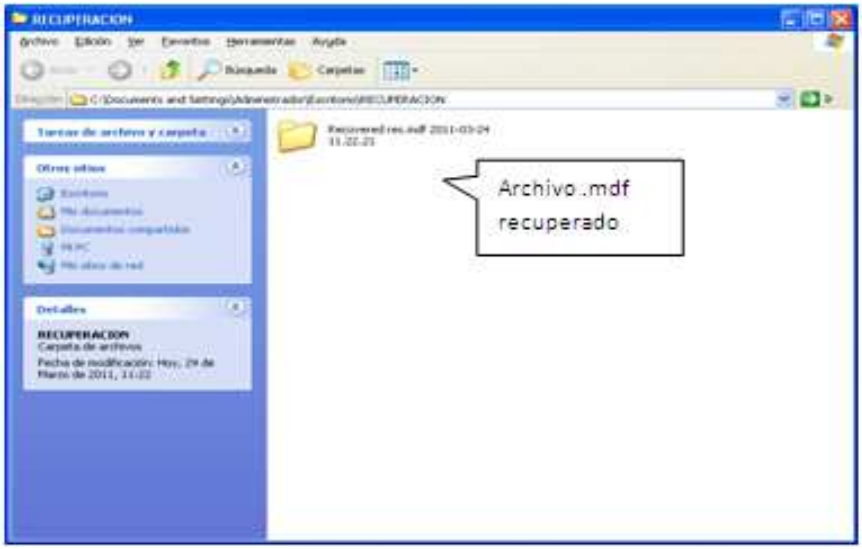


Figura IV.90. Archivo .mdf recuperado

Dentro de la carpeta se encuentra la información recuperada.

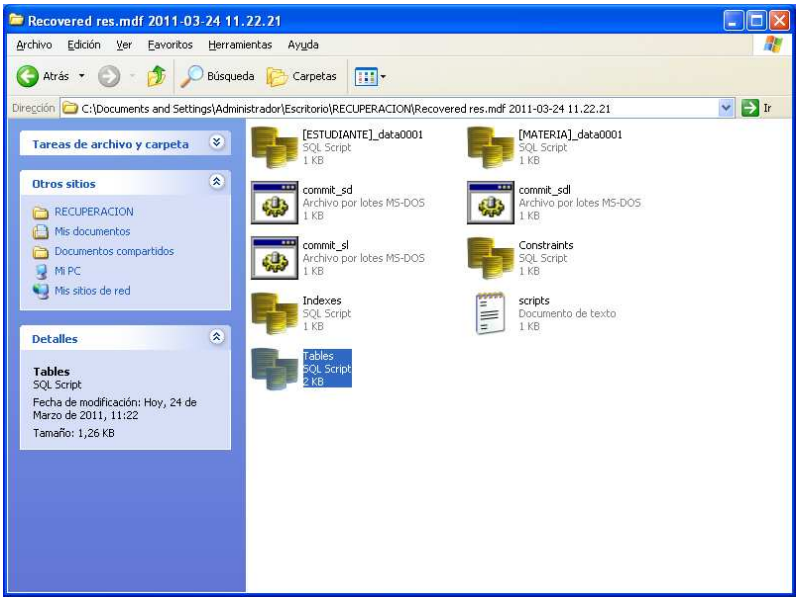


Figura IV.91. Información recuperada

Tabla IV.IX Cuadro Resumen de Herramientas de Recuperación de Base de Datos

HERRAMIENTA	REQUISITOS DEL SISTEMA	LICENCIA	TIPO DE RECUPERACION
RECOVERY FOR MY SQL VERSION 2.0	**Sistema operativo:** Windows 2000, XP, Vista, 2003 Server o 2008 Server. Windows 95, 98, ME no son compatibles. **RAM**: 256-1024 MB (depende del tamaño de la base de datos y la corrupción rango) **Disco duro:** mínimo 10 MB de espacio libre necesario para la instalación de **Pantalla:** 640 x 480 o mayor resolución, 256 colores	**Licencia Standard:** $ 149,00. **Licencia Enterprise:** $ 223,00. **1 año de Servicio de Licencia:** $ 253,00.	No se recupera claves y tiene limitaciones
ACRONIS RECOVERY FOR MS SSQL SERVER VERSION 1.0	**Plataformas admitidas:** - x86, x64 **Sistemas operativos compatibles:** - Windows 2000 (SP4+) - Windows XP (SP1+) - Windows Vista - Windows Server 2003 (versiones de 3 bits y 64 bits)	**Precio por Licencia**: $ 621,78	
STELLAR PHOENIX DATABASE RECOVERY FOR MYSQL VERSION 2.0	**Sistema operativo:** Windows 7, Vista, Server 2003, XP y 2000 **RAM**: 1 GB como mínimo (2 GB recomendado) **Disco duro:** 50 MB de espacio libre en disco	**Licencia de Administrador:** $ 399	
SYSTOOLS SQL RECOVERY VERSION 4.5	**Sistema operativo:** Windows Todos **RAM**: 64 MB RAM **Disco duro:** Mínimo 10 MB de espacio	**Licencia Personal:** $129	Muestra sólo la tabla de nombres y datos de la tabla
STELLAR PHOENIX SQL RECOVERY	**Sistema Operativo:** Windows 7, Server 2008, Vista, Server 2003, Windows XP, y 2000 **Disco duro:** Al menos 50 MB de espacio libre en disco **RAM:** 512 MB como mínimo (2 GB recomendado)	**Licencia para la organización:** $ 399 **Licencia de usuario de segmento académico:** $ 349	
RECOVERY FOR SQL SERVER VERSION 4.1	**Sistema operativo:** Windows 2000, XP, Vista, 2003 Server o 2008 Server. Windows 95, 98, ME no son compatibles. **RAM:** 256-1024 MB (depende de la base de datos, copias de seguridad y tamaño de registro y la corrupción rango) **Disco duro:** mínimo 10 MB de espacio libre necesario para la instalación	**Standard License** $499,00 **Enterprise License** $748,00 **1-año de licencia de servicios** $848,00	Fechas no comprend en el rango de enero, 1900 - Diciembre 31 2199 se puede recup correctamente Orden de las filas en cuadros recuperados pueden diferir de la orden original

4.4. HERRAMIENTAS DE ANÁLISIS FORENSE

Una de las dificultades que se encontrará el investigador a la hora de analizar determinadas evidencias digitales es que los atacantes emplean cada vez herramientas más sigilosas y perfeccionadas para realizar sus asaltos. Por lo tanto no estará de más disponer de un conjunto de herramientas específicas para el análisis de evidencias que nos ayudaran a completar de forma más eficiente nuestra investigación.

Para recolectar evidencias en un incidente que implique la Base de Datos no existen herramientas especificas por ello se utiliza algunas herramientas de investigación forense tradicional y herramientas propias del sistema manejador de base de datos.
A continuación se presenta las herramientas que se va utilizar para nuestra investigación forense en SQL Server 2005.

Helix CD: Esta herramienta pertenece a la categoría de Live CD's. Este tipo de herramientas tienen, entre otras ventajas propias de ellas, que no necesitan tiempo para ser instaladas ni tampoco es necesario cargar otro sistema operativo; de ser necesario, simplemente se inicia la herramienta desde el CD y queda lista para utilizar.
Helix es un Live CD de respuesta ante incidentes, basado en una distribución de Linux llamada Knoppix. Helix contiene una serie de herramientas que permiten realizar análisis forenses de forma efectiva y práctica tanto de equipos de cómputo como de imágenes de discos. La herramienta puede ser descargada directamente de http://www.e-fense.com/helix. La herramienta ofrece dos modos de funcionamiento

- **Entorno Windows**: Contiene un conjunto de herramientas que permiten recuperar la información volátil del sistema.
- **Entorno Linux:** Contiene un sistema operativo completo modificado óptimamente para el reconocimiento de hardware. También está diseñado para no realizar ninguna operación en el disco duro del equipo donde se arranque ya que esto tendría como resultado la pérdida o alteración de la evidencia digital lo cual sería perjudicial y poco deseable para la investigación en curso.

Finalmente es importante resaltar que éste Live CD cuenta, además de los comandos de análisis propios de Linux, con una serie de herramientas forenses importantes como The Sleuthkit & Autopsy

SQLCMD

Es una utilidad para el manejo de bases de datos relacionales (SGBD) basado en el lenguaje Transact-SQL mediante la línea de comandos. SQLCMD utiliza el OLE DB para su conexión con la Base de datos. SQLCMD también es uno de los últimos recursos cuando el sistema falla (por ejemplo cuando la base de datos principal del sistema llamada master se corrompe). Cuando se cuelgue el sistema o no este disponible. La Conexión dedicada de Administración (DAC en inglés) es uno de los últimos recursos.

Utilizando la línea de comandos sqlcmd, usted puede:

- Mandar instrucciones T-SQL a la base de datos SQL Server.
- Crear scripts y procedimientos.
- SQLCMD permite una conexión dedicada de administración utilizando el parámetro -A como sigue: sqlcmd –A
- Permite escribir instrucciones Transact-SQL, procedimientos del sistema y archivos de script en el símbolo del sistema, en el Editor de consultas en modo SQLCMD, en un archivo de script de Windows o en un paso de trabajo del sistema operativo (Cmd.exe) de un trabajo del Agente de SQL Server.

MD5

Es uno de los algoritmos de reducción criptográficos diseñados por el profesor Ronald Rivest del MIT (Massachusetts Institute of Technology, Instituto Tecnológico de Massachusetts). Fue desarrollado en 1991 como reemplazo del algoritmo MD4 después de que Hans Dobbertin descubriese su debilidad.

A pesar de su amplia difusión actual, la sucesión de problemas de seguridad detectados desde que, en 1996, Hans Dobbertin anunciase una colisión de *hash*, plantea una serie de dudas acerca de su uso futuro.

Codificación

La codificación del MD5 de 128 bits es representada típicamente como un número de 32 dígitos hexadecimal. El siguiente código de 28 bytes ASCII será tratado con MD5 y veremos su correspondiente *hash* de salida:

MD5 ("Esto sí es una prueba de MD5") = e99008846853ff3b725c27315e469fbc

Un simple cambio en el mensaje nos da un cambio total en la codificación *hash*, en este caso cambiamos dos letras, el «sí» por un «no».

MD5 ("Esto no es una prueba de MD5") = dd21d99a468f3bb52a136ef5beef5034

Otro ejemplo sería la codificación de un campo vacío:

MD5 ("") = d41d8cd98f00b204e9800998ecf8427e

Windows Forensic Toolchest™ (WFT) está diseñado para proporcionar un enfoque estructurado y repetible automatizado de una consulta Forense en vivo, respuesta a incidentes, auditoría o en un sistema Windows durante la percepción de seguridad de la información relevante del sistema.

WFT es esencialmente un shell de procesamiento por lotes forense mejorada capaz de ejecutar otras herramientas de seguridad y producción de informes basados en HTML de manera forense de sonido.

Un profesional de la seguridad bien informado puede usar WFT para ayudar a buscar señales de un incidente, de intrusos, o para confirmar el mal uso de equipo de configuración. WFT produce una salida que sea útil para el usuario admin, pero también es apropiado para su uso en los procedimientos judiciales. Se ofrece un amplio registro de todas sus acciones, junto con el cálculo de valores de hash MD5/SHA1, lo que permite asegurarse de que su salida es verificable.

La principal ventaja de usar WFT para llevar a cabo las respuestas de incidentes o de auditoría es que proporciona una forma simplificada de scripting esas actividades utilizando una metodología adecuada para la recogida de datos.

Beneficios de WFT

Proporcionar una respuesta que es:

- Consistente y verificable

- Metodología Forense sólida
- Minimiza los impactos del sistema
- Aplica binarios conocidos
- Visualmente atractivo (HTML presentación de informes)
- Utiliza la memoria en uso y lee un par de entradas en el registro, ya que se compila con Visual C + +, pero no mucho más).

Configuración de Windows Forensic Toolchest

Para esta investigación en particular se debe realizar una configuración personalizada, que permita la recolección de evidencias en SQL Server 2005, para eso se debe seguir los siguientes pasos:

1. Download wft.exe (versión: v3.0.05) desde / http://www.foolmoon.net/security/
2. Crear una carpeta IR en el escritorio.
3. Copiar dentro de la carpeta IR la carpeta WFT.
4. Copiar bajo Tools todos los archivos de WFT.
5. Crear una carpeta SQL dentro de Tools y pegar estos tres archivos (sqlcmd.exe, Batchparser90.dll, sqlcmd.rll).
6. Copiar los archivos *WFTSQL.bat* and *WFTSQL.cfg* dentro de la carpeta wft.
7. Copiar cmd.exe dentro de la carpeta Tools este archivo cambiara dependiendo del sistema operativo.
8. Copiar dentro de la carpeta SQL los script de SQL Server Incident Response.
9. Download RunSQL.bat y copiar dentro de la carpeta SQL.
10. Luego configurar el archivo WFTSQL.cfg y reemplazar por el archivo existente wftsql.cfg con la nueva configuración.
11. Una vez configurados los archivos ejecutar el archivo wftSQL.bat.
12. Ingresar la instancia del SQL SERVER.

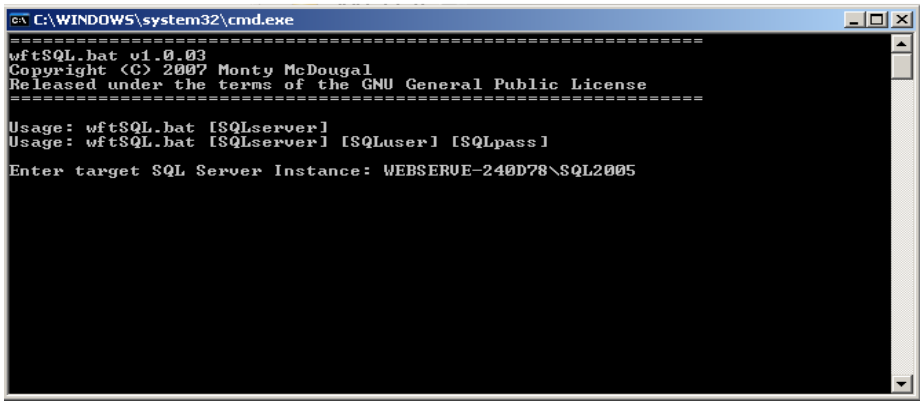


Figura IV.92. Ingresar instancia de SQL Server 2005

13. Ingresar *Y*, si el usuario SQL server usa credenciales caso contrario ingresar *N*.

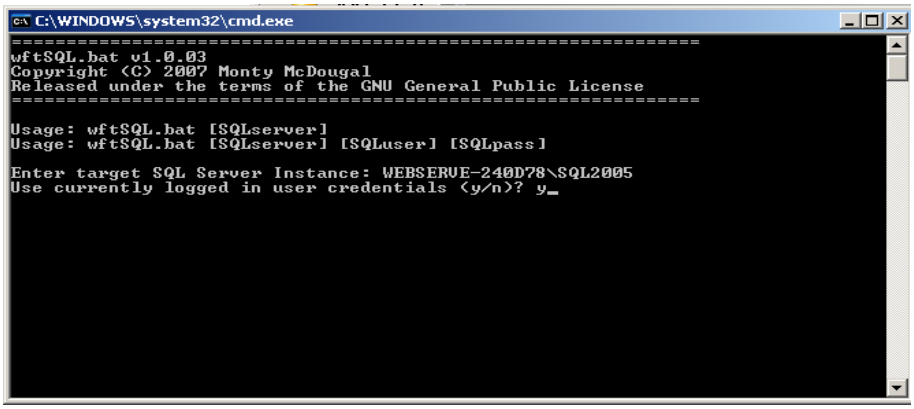


Figura IV.93. Indicar si utiliza o no credenciales

14. El archivo ejecutara la aplicación.

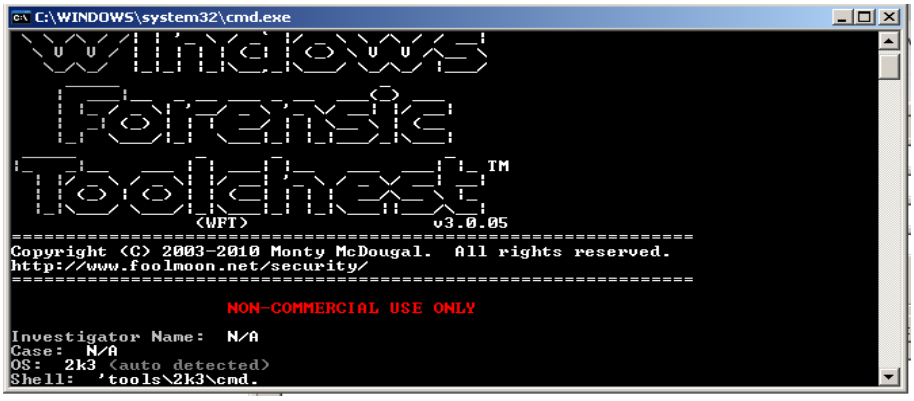


Figura IV.94. Ventana inicial Windows Forensic Toolchest

15. Si el archivo esta bien configurado el programa cargara todos los archivos de la siguiente manera.

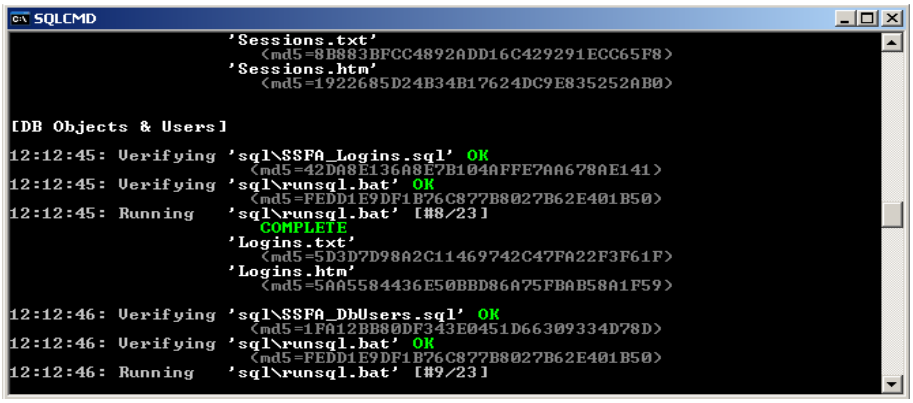


Figura IV.95. Ejecución de sentencias SQL Server

16. Completada la ejecución del programa, esta dara como resultado un documento index.htm.

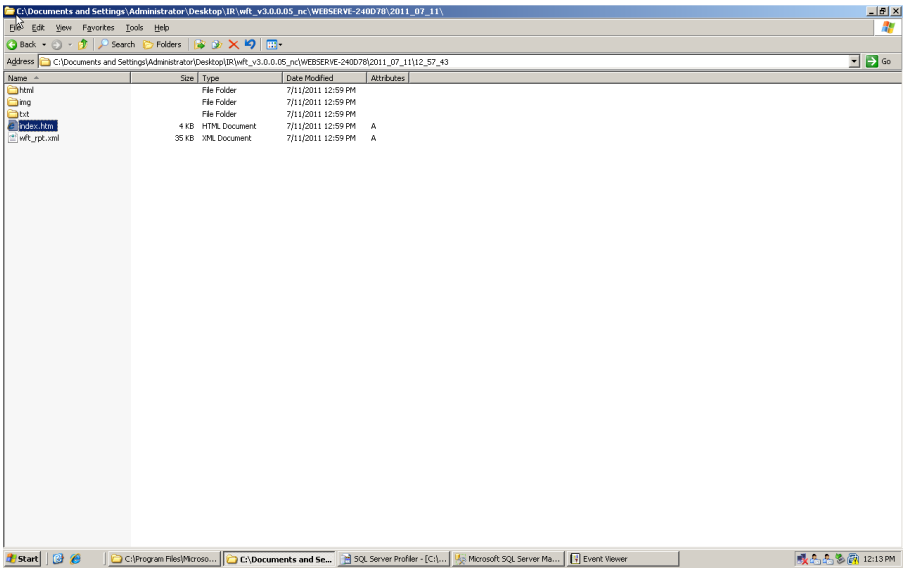


Figura IV.96. Carpeta con resultados del análisis forense

17. En el documento html se encuentra toda la información del sistema y del servidor de base de datos.

Figura IV.97. Información del Sistema

4.5. ANÁLISIS COMPARATIVO DE LAS HERRAMIENTAS DE REPARACIÓN Y RECUPERACIÓN DE BASES DE DATOS

Tabla IV.X Cuadro Resumen de Herramientas de Recuperación de Base de Datos

HERRAMIENTA	FACILIDAD DE USO	OBTECIÓN DE LA HERRAMIENTA	FUNCIONALIDAD	TIPO DE RECUPERACIÓN											
				RECUPERA ARCHIVOS(.mdf, .myi, .myd)		Restaura la estructura de la tabla y los datos		Recupera y realiza copias de seguridad		Recuperación automática al punto de error		Recupera procedimientos almacenados, vistas, índices, password, etc,		Cree un plan de recuperación de catástrofes	
				TIEMPO	RECUPERO INFO (SI/NO)	TIEMPO	RECUPERO INFO (SI/NO)	TIEMPO	RECUPERO INFO (SI/NO)	TIEMPO	RECUPERO INFO (SI/NO	TIEMPO	CANT INF(%)	TIEMPO	RECUPERO INFO (SI/NO
Acronis Recovery For Ms Sql Server	85%	Pagado	80%	5 min	SI	10 min	SI	20 min	SI	20 min	SI	10 min	100	20 min	SI
Systools Sql Recovery	85%	Pagado	75%	5 min	SI	10 min	SI	25 min	SI	-	No	10 min	100	-	No
Stellar Phoenix Sql Recovery	90%	Pagado	70%	4 min	SI	15 min	SI	20 min	SI	20 Min	SI	15 min	100	20 min	SI
Recovery For Sql Server	85%	Pagado	75%	5 min	SI	15 min	SI	20 min	SI	-	No	15 min	100	-	No
Recovery For My Sql	75%	Pagado	75%	8 min	SI	10 min	SI	20 min	SI	-	No	10 min	90	-	No
Stellar Phoenix Database Recovery For Mysql	75%	Pagado	75%	8 min	SI	10 min	SI	20 min	SI	20 min	SI	10 min	100	20 min	SI

Conclusiones

- Todas las herramientas de reparación de base de datos analizadas son pagadas, lo cual dificulta un poco el análisis de éstas ya que los demos tienen limitaciones.
- Stellar Phoenix Sql Recovery y Acronis Recovery For Ms Sql Server crean un plan de recuperación de catástrofes para SQL Server.
- Stellar Phoenix Database Recovery For Mysql crea un plan de recuperación de catástrofes para el servidor de datos Mysql.

DETALLES DE LOS PARÁMETROS DE ANÁLISIS DE LAS HERRAMIENTA DE RECUPERACIÓN

Análisis con SQL Server

Tabla II.XI Cantidad de Información de Herramientas de Recuperación de Base de Datos con SQL Server

PARÁMETROS / HERRAMIENTAS	UBICACIÓN	NÚMERO DE TABLAS A RECUPERAR	NÚMERO DE TABLAS RECUPERADAS	TOTAL (%)
ACRONIS RECOVERY FOR MS SQL SERVER	Diferentes	8	8	100
SYSTOOLS SQL RECOVERY	Diferentes	8	7	87,5
STELLAR PHOENIX SQL RECOVERY	Diferentes	8	7	87,5
RECOVERY FOR SQL SERVER	Diferentes	8	7	87,5

Fuente: Análisis práctico realizado en la Tesis

Elaborado por: Nancy Macas

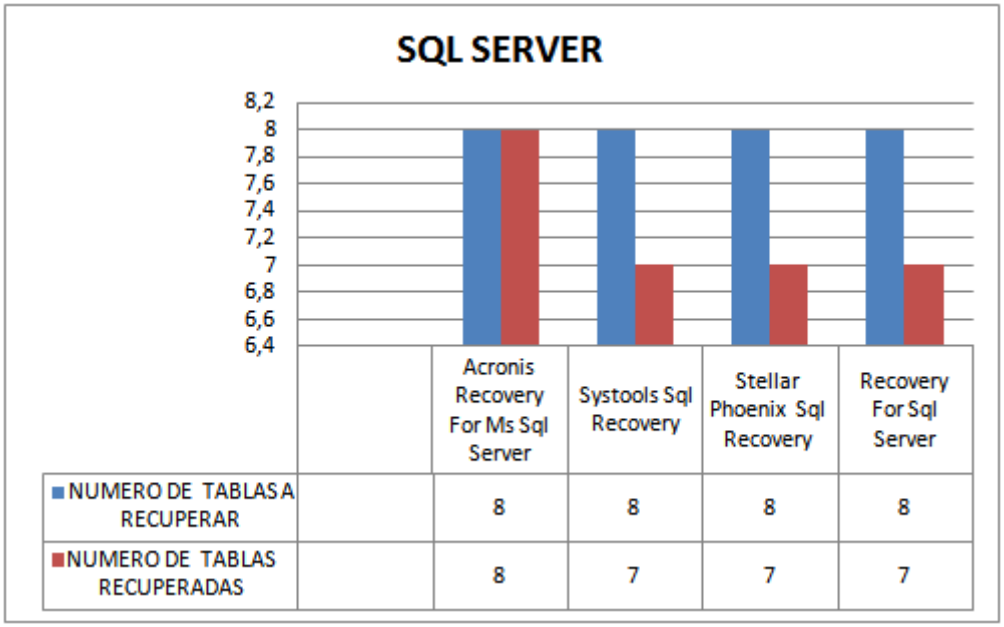


Figura IV.98. Resultados de análisis de herramientas de recuperación en SQL SERVER

Conclusión

Acronis Recovery For Ms SQL Server es la mejor herramienta en cuanto se refiere a la cantidad de información recuperada para SQL Server.

Análisis con Mysql

Tabla IV.XII Cantidad de Información de Herramientas de Recuperación de Base de Datos con MySQL

PARÁMETROS / HERRAMIENTAS	UBICACIÓN	NÚMERO DE TABLAS A RECUPERAR	NÚMERO DE TABLAS RECUPERADAS	TOTAL (%)
RECOVERY FOR MY SQL	Diferentes	8	7	87,5
STELLAR PHOENIX DATABASE RECOVERY FOR MYSQL	Diferentes	8	8	100

Fuente: Análisis práctico realizado en la Tesis

Elaborado por: Nancy Macas

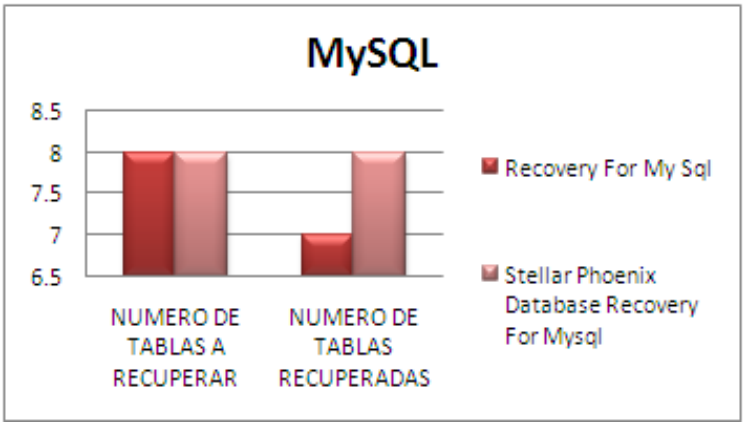


Figura IV.99. Resultados de análisis de herramientas de recuperación en MySQL

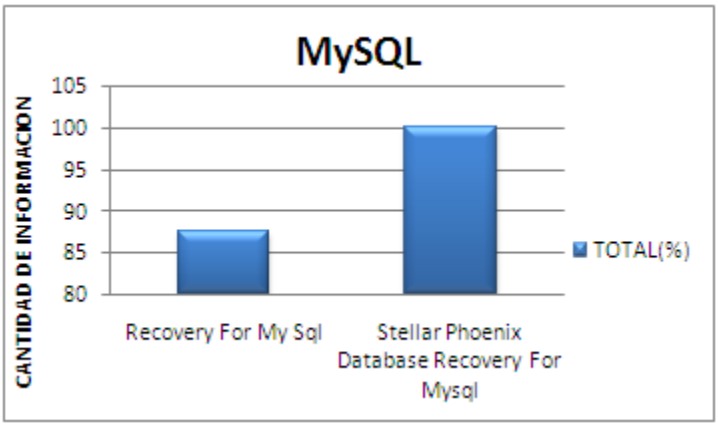


Figura IV.100. Resultados totales de cant. Información recuperada de la herramienta de recuperación en MySQL

Conclusión

Stellar Phoenix Database Recovery For Mysql es una buena herramienta para recuperar la mayor cantidad de información en Mysql.

Matriz Facilidad de Uso

Valoración

1= COMPLICADO (requiere de conocimientos)

2= MEDIO (conocimientos básicos)

3=FACIL (intuitivo)

Análisis en SQL Server

Tabla IV.XIII Facilidad de Uso de Herramientas de Recuperación de Base de Datos Con SQL Server

PARAMETROS / HERRAMIENTAS	INSTALACION	MANEJO	INTERFAZ	TOTAL (SUMA)	TOTAL (%)
ACRONIS RECOVERY FOR MS SQL SERVER	3	3	3	9	100
SYSTOOLS SQL RECOVERY	3	3	3	9	100
STELLAR PHOENIX SQL RECOVERY	3	3	3	9	100
RECOVERY FOR SQL SERVER	3	3	3	9	100

Fuente: Análisis práctico realizado en la Tesis

Elaborado por: Nancy Macas

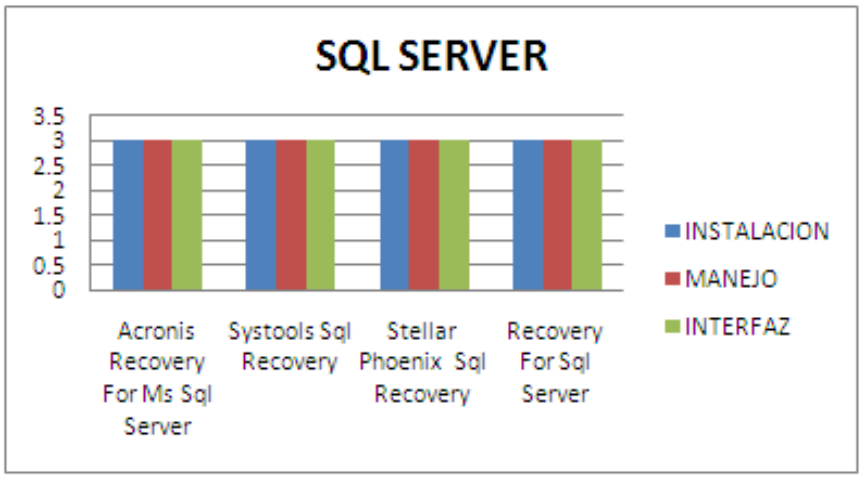


Figura IV.101. Resultados Facilidad de Uso en SQL Server

Conclusión

Las herramientas utilizadas para la recuperación de base de datos son fáciles de utilizar ya que cuentan con una buena interfaz lo cual permiten al usuario un excelente manejo

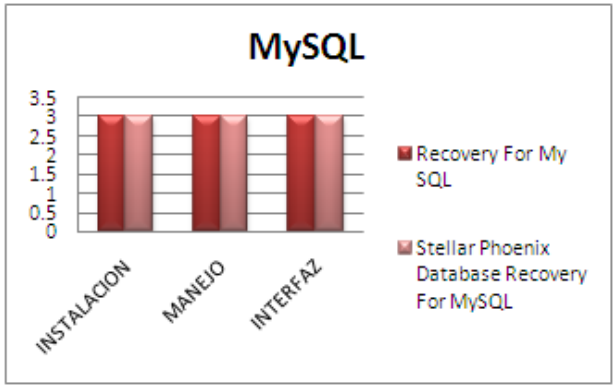
Análisis en MySQL

Tabla IV.XIV Facilidad de Uso de Herramientas de Recuperación de Base de Datos con MySQL

PARÁMETROS / HERRAMIENTAS	INSTALACIÓN	MANEJO	INTERFAZ	TOTAL (SUMA)	TOTAL (%)
RECOVERY FOR MY SQL	3	3	3	9	100
STELLAR PHOENIX DATABASE RECOVERY FOR MYSQL	3	3	3	9	100

Fuente: Análisis práctico realizado en la Tesis

Elaborado por: Nancy Macas



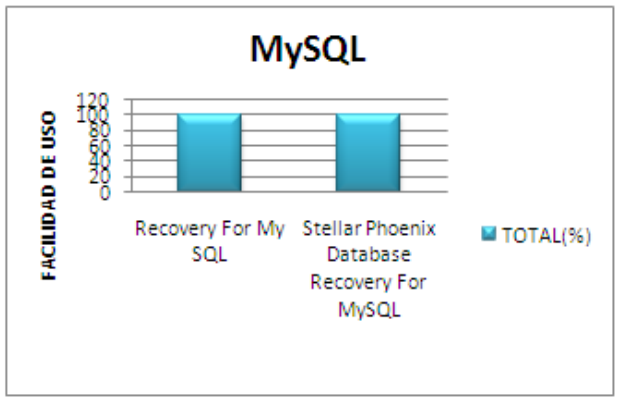


Figura IV.102. Resultados Facilidad de Uso en MySQL

Conclusión

La facilidad de uso de estas herramientas es totalmente fácil ya que cuentan con una interfaz amigable.

Matriz Funcionalidad

Valoración

√ SI

X NO

Los parámetros se realizan en base a la recuperación que ejecutan las herramientas ya sea si se borro o restaura algún elemento de la base de datos.

Análisis en SQL Server

Tabla IV.XV Funcionalidad de Herramientas de Recuperación de Base de Datos en SQL Server

PARÁMETROS / HERRAMIENTAS	Recupera archivos(.mdf)	Restaura la estructura de la tabla y los datos	Recupera y realiza copias de seguridad	Recuperación automática al punto de error	Recupera procedimientos almacenados, vistas, índices, etc	Cree un plan de recuperación de catástrofes	TOTAL (%)
ACRONIS RECOVERY FOR MS SQL SERVER	√	√	√	√	√	√	100
SYSTOOLS SQL RECOVERY	√	√	√	X	√	X	66,66
STELLAR PHOENIX SQL RECOVERY	√	√	√	√	√	√	100
RECOVERY FOR SQL SERVER	√	√	√	√	√	X	83,33

Fuente: Análisis práctico realizado en la tesis

Elaborado por: Nancy Macas

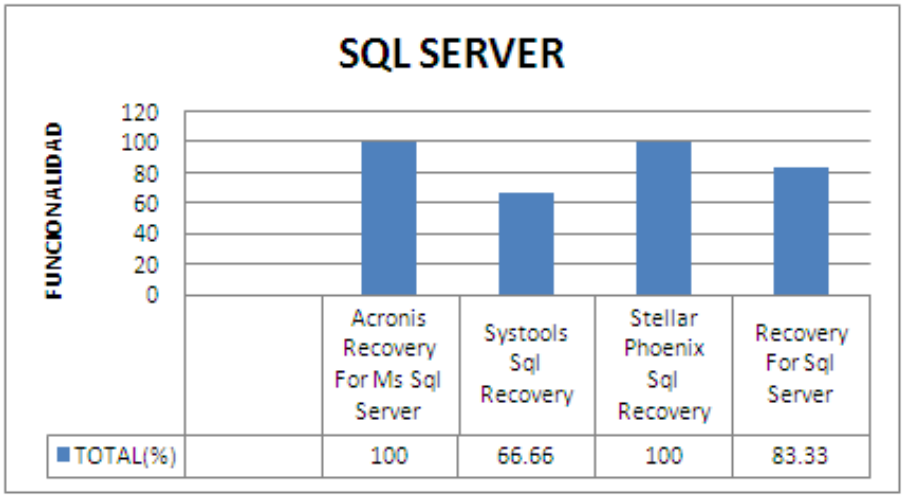


Figura IV.103. Resultados Funcionalidad SQL SERVER

Conclusión

Acronis Recovery For Ms Sql Server y Stellar Phoenix Sql Recovery Server son herramientas que nos brindan mayor número de funcionalidades logrando una mejor recuperación y reparación de la base de datos.

Análisis con MySQL

Tabla IV.XVI Funcionalidad de Herramientas de Recuperación de Base de Datos en MySQL

PARÁMETROS / HERRAMIENTAS	RECUPERA ARCHIVOS(.myi, .myd)	Restaura la estructura de la tabla y los datos	Recupera y realiza copias de seguridad	Recuperación automática al punto de error	Recupera procedimientos almacenados, vistas, índices, etc	Cree un plan de recuperación de catástrofe	TOTAL (%)
RECOVERY FOR MY SQL	✓	✓	✓	X	✓	X	66,66
STELLAR PHOENIX DATABASE RECOVERY FOR MYSQL	✓	✓	✓	✓	✓	✓	100

Fuente: Análisis práctico Realizado en la Tesis

Elaborado por: Nancy Macas

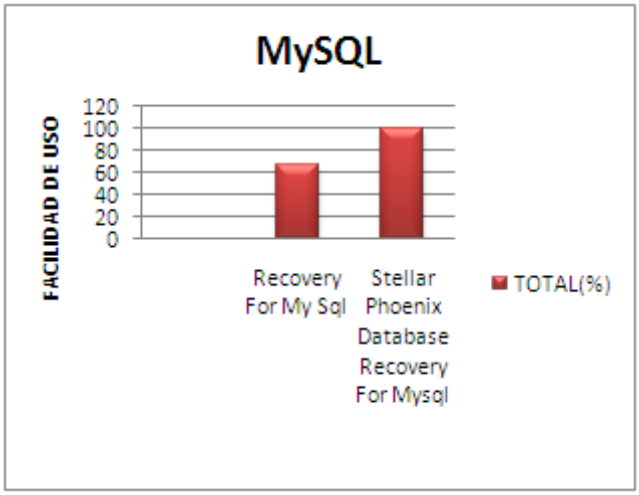


Figura IV.104. Resultados Funcionalidad MySQL

Conclusión

Stellar Phoenix Database Recovery For Mysql tiene un 100% de funcionalidad para reparar bases de datos My Sql

Resultados del Análisis de las Herramientas de Reparación y Recuperación de Base de Datos

- Las herramientas Stellar Phoenix Sql Recovery y Acronis Recovery For Ms Sql Server son las que mayor beneficios nos brindan para servidores de datos SQL Server
- Stellar Phoenix Database Recovery For Mysql es una gran alternativa para trabajar con MySql

4.6. ANÁLISIS COMPARATIVO DE LAS HERRAMIENTAS DE DETECCIÓN DE VULNERABILIDADES

Tabla IV.XVII Tabla Comparativa de Herramientas de Detección de Vulnerabilidades en Base de Datos

PARÁMETROS / HERRAMIENTAS	FACILIDAD DE USO		OBTENCION DE LA HERRAMIENTA	FUNCIONALIDAD	DETECCIÓN DE VULNERABILIDADES	
	SQL Server	MySQL			SQL Server	MySQL
ACUNETIX WEB VULNERABILITY SCANNER	100%	-	Pagado	60%	60%	-
HAVIJ	100%	100%	Libre	60%	100%	100%
NGSSQUIRREL	100%	-	Pagada	80%	80%	-
N-STALKER	88,90%	-	Pagado	60%	80%	-
SQLRECON	100%	-	Pagada	60%	60%	-
WEBCRUISER	88,90%	88,90%	Pagado	80%	80%	80%

Fuente: Análisis práctico realizado en la Tesis.

Elaborado por: Ana Juntamay

Detalles de los Parámetros de la Comparativa de Herramientas de Detección de Vulnerabilidades en Base de Datos

Matriz Facilidad de Uso

Valoración

1= COMPLICADO (requiere de conocimientos)

2=MEDIO (conocimientos básicos)

3=FACIL (intuitivo)

Análisis con SQL Server

Tabla IV.XVIII Facilidad de Uso de Herramientas de Detección de Vulnerabilidades en Base de Datos con SQL Server

PARÁMETROS / HERRAMIENTAS	INSTALACIÓN	MANEJO	INTERFAZ	TOTAL (SUMA)	TOTAL (%)
ACUNETIX WEB VULNERABILITY SCANNER	3	3	3	9	100
HAVIJ	3	3	3	9	100
NGSSQUIRREL	3	3	3	9	100
N-STALKER	3	2	3	8	88,90
SQLRECON	3	3	3	9	100
WEBCRUISER	3	2	3	8	88,90
PROMEDIO	3	2,67	3	8,67	96,3

Fuente: Análisis práctico realizado en la tesis.

Elaborado por: Ana Juntamay

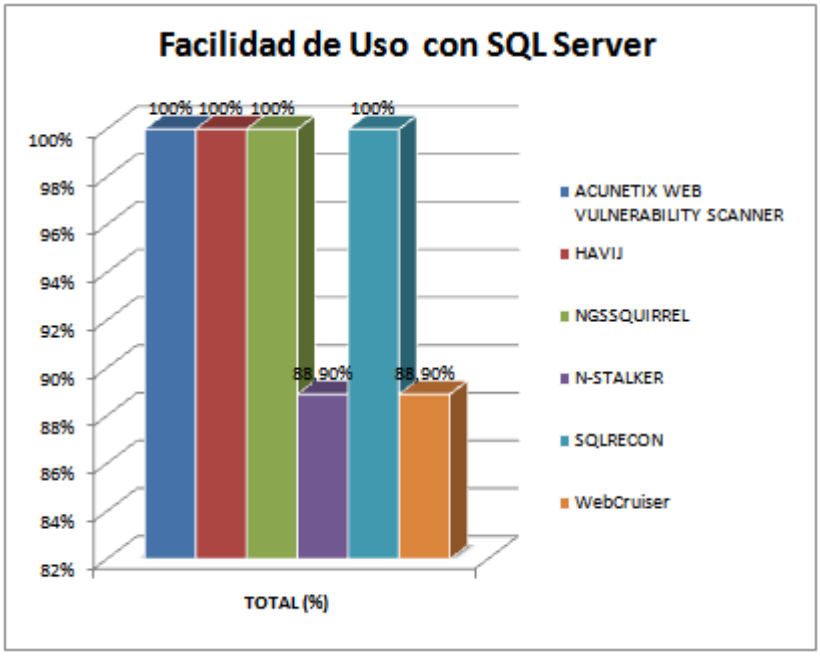


Figura IV.105. Herramientas de Detección de Vulnerabilidades en Función de la Facilidad de Uso con SQL Server

Conclusión

En cuanto a la facilidad de uso la mayoría de escáners son fáciles de usar y sobre todo son intuitivos, sin embargo en cuanto al manejo se puede mencionar que WebCruiser y N-Stalker necesitan mayor nivel de conocimientos técnicos para su óptima utilización.

Análisis con MySQL

Tabla IV.XIX Facilidad de Uso de Herramientas de Detección de Vulnerabilidades en Base de Datos con MySQL

PARÁMETROS / HERRAMIENTAS	INSTALACION	MANEJO	INTERFAZ	TOTAL (SUMA)	TOTAL (%)
HAVIJ	3	3	3	9	100
WEBCRUISER	3	2	3	8	88,90
PROMEDIO	3	3	3	8,5	94,50

Fuente: Análisis práctico realizado en la Tesis

Elaborado por: Ana Juntamay

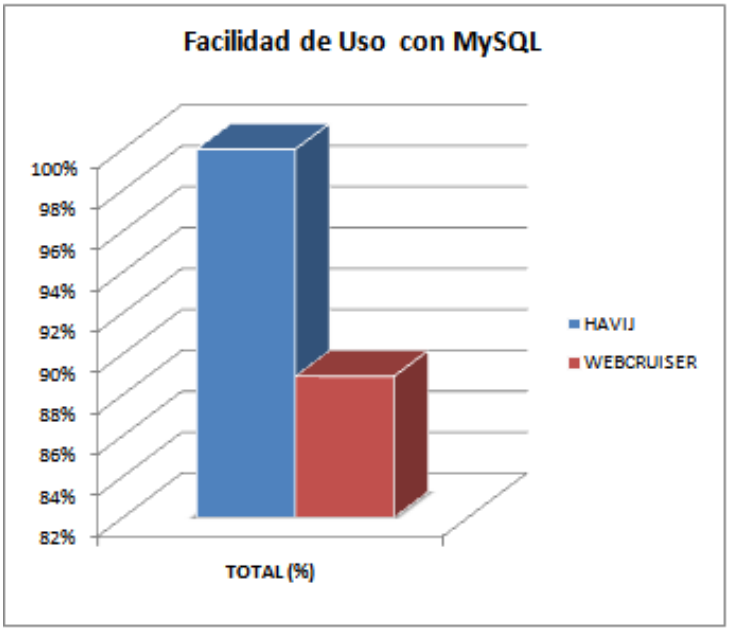


Figura IV.106. Herramientas de Detección de vulnerabilidades en función de la Facilidad de Uso con MySQL

Conclusión

Havij es la mejor herramienta en cuanto a facilidad de uso, mientras que WebCruiser en cuanto al manejo requiere mayor conocimiento técnico.

Matriz Funcionalidad

Valoración

√ SI

X NO

Análisis con SQL Server y MySQL

Tabla IV.XX. Funcionalidad de las Herramientas de Detección de Vulnerabilidades en Base de Datos con SQL Server y MySQL

PARÁMETROS / HERRAMIENTAS	Incluye visualización de reportes	Permite escaneo mediante host	Permite escaneo mediante rangos de IP	Trabaja con SQL Server	Trabaja con MySQL	TOTAL (%)
ACUNETIX WEB VULNERABILITY SCANNER	√	√	X	√	X	60
HAVIJ	X	√	X	√	√	60
NGSSQUIRREL	√	√	√	√	X	80
N-STALKER	√	√	X	√	X	60
SQLRECON	X	√	√	√	X	60
WEBCRUISER	√	√	X	√	√	80
PROMEDIO	66.67	100	33.33	100	33.33	66.67

Fuente: Análisis práctico realizado en la tesis.

Elaborado por: Ana Juntamay

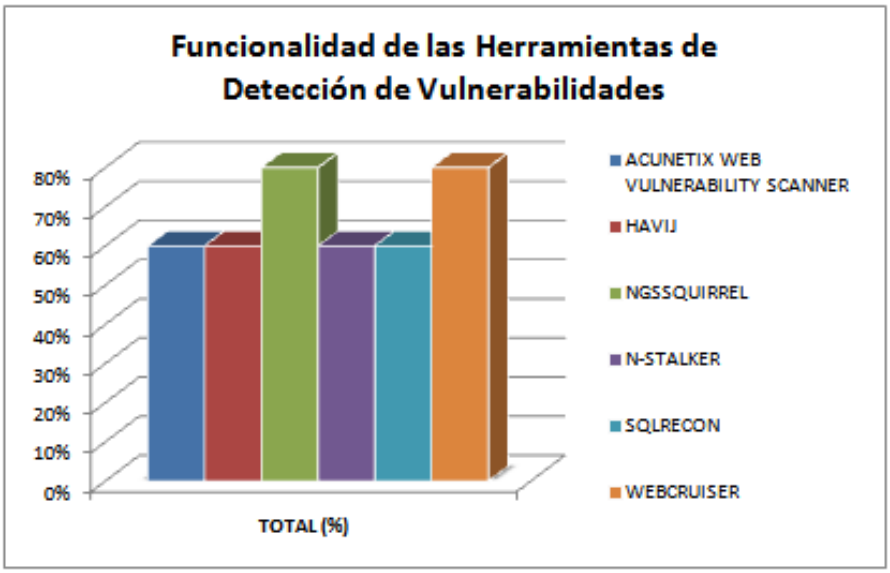


Figura IV.107. Funcionalidad de Herramientas de Detección de Vulnerabilidades en Base de Datos con SQL Server y MySQL

Conclusión

Las mejores herramientas son NGSSQuirrel y WebCruiser porque le ofrece una funcionalidad alta, además ofrece características excelentes y acceso a mayor información del DBMS.

Tabla IV.XXI Detección de Vulnerabilidades en Base de Datos con SQL Server

VULNERABILIDADES / HERRAMIENTAS	Inyección SQL	Puertos Abiertos	Contraseñas débiles	Acceso a elementos de la BD (tablas, procedimientos, vistas, etc.)	Otros (Framework, Memoria, etc)	TOTAL (%)
ACUNETIX WEB VULNERABILITY SCANNER	√	√	X	X	√	60
HAVIJ	√	√	√	√	√	100
NGSSQUIRREL	X	√	√	√	√	80
N-STALKER	√	√	√	X	√	80
SQLRECON	X	√	√	√	X	60
WEBCRUISER	√	√	X	√	√	80
PROMEDIO	66.67	100	66.67	66.67	83.33	76.68

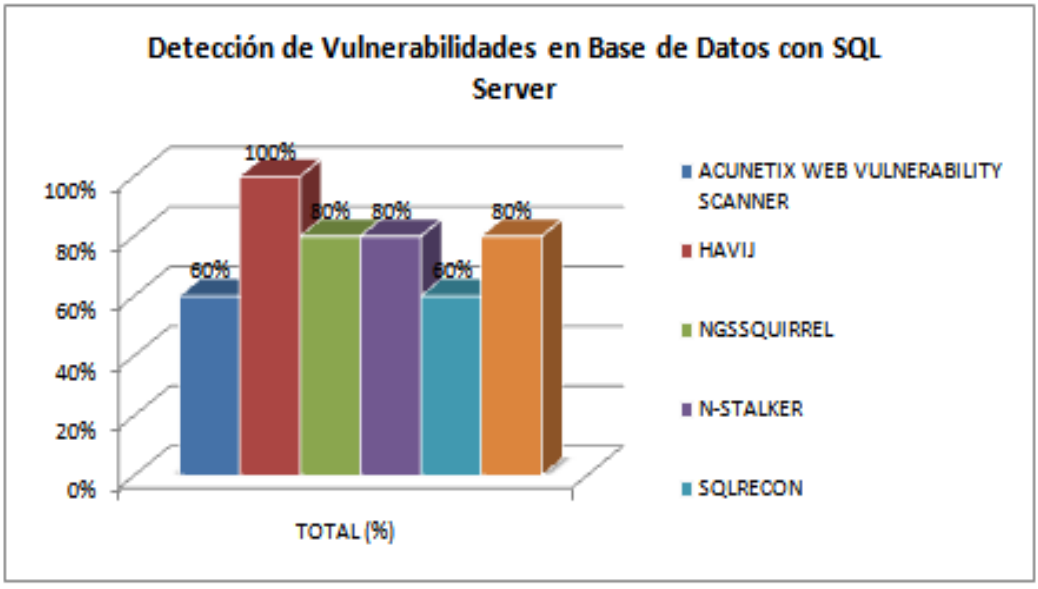


Figura IV.108. Resultados de la detección de Vulnerabilidades en SQL Server

Conclusión

La mejor herramienta es Havij ya que permite detectar algunas vulnerabilidades, a continuación están NGSSQuirrel, N-Stalker y WebCruiser que permiten visualizar los elementos de la Base de Datos.

Tabla IV.XXII Detección de Vulnerabilidades en Base de Datos con MySQL

VULNERABILIDADES / HERRAMIENTAS	Inyección SQL	Puertos Abiertos	Contraseñas Débiles	Acceso a elementos de la BD (tablas, procedimientos, vistas, etc.)	Otros (Framework, Memoria, etc)	TOTAL (%)
HAVIJ	√	√	√	√	√	100
WEBCRUISER	√	√	X	√	√	80
PROMEDIO	100	100	50	100	100	90

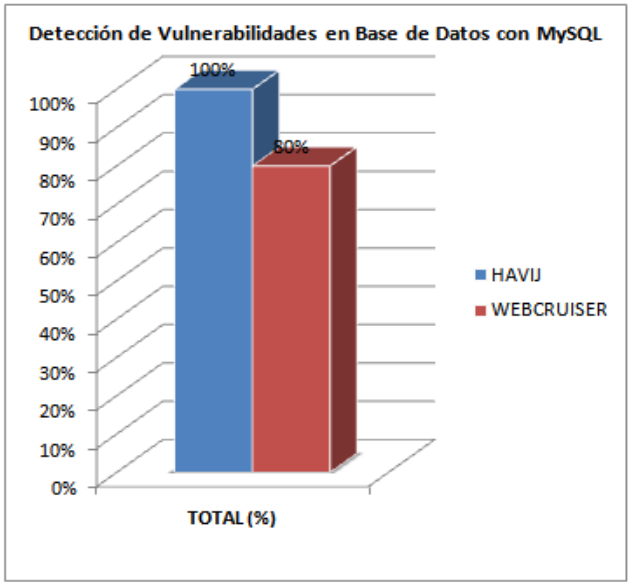


Figura IV.109. Resultados de la detección de Vulnerabilidades en MySQL

Conclusión

La mejor herramienta es Havij ya que le permite trabajar con inyección ciega y otras opciones para acceder a los datos almacenados en MySQL.

CAPÍTULO V

PROPUESTA DE LA GUíA DE TÉCNICAS Y PROCEDIMIENTOS DE ANÁLISIS FORENSE EN UNA BASE DE DATOS

5.1. INTRODUCCIÓN

Hoy en día los servidores de base de datos almacenan información sensible y crítica que representan un alto coste para una institución o empresa. Las infracciones contra la seguridad de la base de datos son cada día más frecuentes. Sin embargo las investigaciones tradicionales a menudo excluyen las bases de datos.

El principal elemento que se debe proteger en una investigación de cualquier tipo que involucre un servidor de base de datos es el equipo en el que se encuentra instalada la aplicación. Es en éste que se encuentra la posible evidencia digital que puede llegar a ser determinante en un caso judicial. La evidencia digital, debido a su naturaleza, es extremadamente frágil. Basado en lo anterior, es sobresaliente seguir un procedimiento estándar que asegure la protección y el análisis exitoso de dicha evidencia digital con el fin de encontrar la mayor cantidad de detalles sobre el incidente ocurrido en el equipo, sin embargo, para diseñar lo anterior es necesario revisar con más detenimiento los

procedimientos y estándares establecidos en la actualidad para considerar las mejores prácticas y fases expuestas, generando con ello una guía práctica y fácil de seguir.

5.2. REVISIÓN DE PROCEDIMIENTOS DE ANÁLISIS FORENSE

Por lo que hemos visto en el capítulo III existen una serie de modelos de procedimientos que incluyen no solo el aseguramiento de la evidencia sino todos los pasos y fases que se deben tener en cuenta para realizar análisis forenses.

TheElectronicCrimeSceneInvestigation - A Guide forFirstResponders, propuesto por el departamento de Justicia de Estados Unidos, ofrece los siguientes lineamientos cuando se manipula evidencia digital (14):

- **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 convenciónal.
- **Recolección de evidencia:** Se debe recolectar tanto la evidencia tradiciónal como la digital de manera que se conserve el valor de dicha evidencia.
- **Empaque, transporte y almacenamiento:** Se deben tomar las precauciónes adecuadas cuando se empaque, transporte y almacene la evidencia, manteniendo la cadena de custodia.

Para finalizar, se expone a continuación las prácticas establecidas en el HB171:2003 HandbookGuidelinesforthemanagement of IT evidence desarrollado en Australia y explicado detalladamente en el documento “Buenas prácticas en la administración de la evidencia digital” (5).

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” (5). El ciclo de vida para la administración de evidencia digital consta de seis pasos a saber:

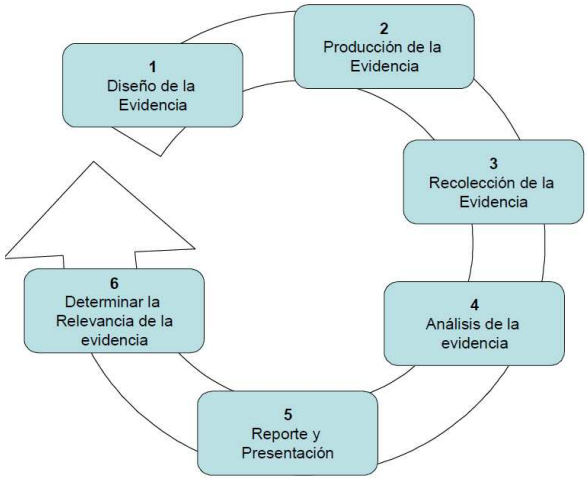


Figura V.110. Ciclo de vida para la Administración de la Evidencia

A continuación de enumeran las seis fases del ciclo de vida y se proporciona una pequeña descripción de cada una (5):

- **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 modelos estándares y procedimientos más aceptados en cuanto a informática forense se refiere, se procede a continuación a proponer una guía de técnicas y procedimientos para realizar análisis forenses orientados a incidentes en servidores de base de datos, 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 servidor de base de datos, se procede a describir la guía propuesta.

5.3. ALCANCE Y LIMITACIÓNES DE LA GUÍA PROPUESTA

Alcance

Existen diversos modelos propuestos para guiar el proceso forense digital en muchas partes del mundo, tal como se presentó en el Capítulo III. Sin embargo, no se ha llegado a ninguna conclusión sobre cuál es la más apropiada. A pesar de que, cada marco de trabajo podría trabajar bien con un tipo de investigación particular, ninguna de ellas se centra en la información específica que está involucrada en el análisis forense de una base de datos. La guía propuesta ha sido desarrollada para ayudar a las prácticas forenses que involucren un Servidor de base de datos.

Se han incorporado aquellas prácticas y técnicas estándar existentes en el mundo de la investigación física y digital. Este modelo intenta superar las principales deficiencias de

los modelos digitales forenses existentes discutidos en las secciones anteriores ya que a menudo estos modelos suelen ser muy generales y excluyen el análisis de la base de datos atacada.

Limitaciones

La guía presenta las siguientes limitaciones:

- El alcance de la guía está limitada a servidores de base de datos SQL Server 2005 y MySQL 5.x.

5.4. CARACTERÍSTICAS DE LA GUÍA PROPUESTA

La guía de procedimiento propuesta presenta las siguientes características:

Modular.- se divide en seis fases cada una de ellas se complementa para realizar un correcto análisis forense

Consistente.- se fundamenta en escenarios reales

Es de aplicación limitada.- Es complicado que un modelo puede atender o resolver todas las posibles circunstancias que pudieran generarse en un momento determinado. Por lo tanto, la guía propuesta también presenta limitaciones al momento de su aplicación

Verificable.- las evidencias y resultados obtenidos pueden ser sometidos a pruebas

Organizado.- la guía de procedimientos presenta sus fases en un orden el cual es recomendable seguirlo

Incremental.-Las fases se realizar de forma secuencial, aunque dependiendo del tipo de evidencias que tengamos en escena (volátiles o no volátiles) habrá un tratamiento distinto, esencialmente en cuestión de rapidez de la recolección de evidencias digitales.

Respaldo Legal.- los resultados del informe pueden establecer casos ilícitos informáticos

5.5. FASES DE LA GUÍA PROPUESTA

Debido a que cada investigación es distinta con su propio y único conjunto de circunstancias, un enfoque de procedimiento definitivo es complicado establecer. A

pesar de todo, varias propuestas hacen referencia a las mismas áreas, aunque resaltan el grado de importancia en aspectos diferentes.

La guía aquí propuesta está orientada a ser empleada en aquellos incidentes o delitos en los que se requiera obtener evidencia digital de una base de datos que estuviera involucrada. La guía propuesta se estructuró en 6 fases. Las cuales están complementadas de tal forma, que permitan incluir la mayor cantidad de puntos a considerar para realizar el proceso de análisis forense a servidores de base de datos SQL Server y MySQL y se explican a continuación.

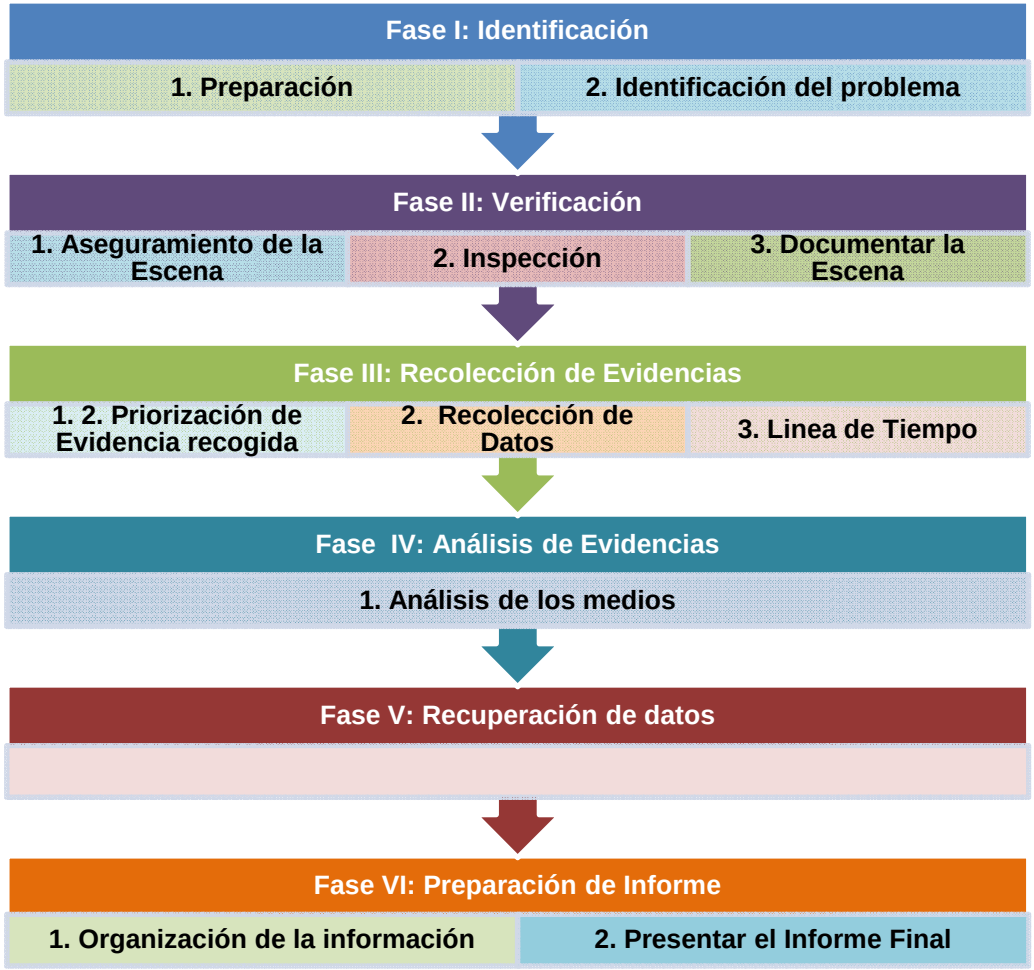


Figura V.111. Fases de la Guía de Análisis Forense Propuesta

Ahora que se cuenta con el listado de fases, es posible presentar una comparación entre las actividades de la guía propuesta con las actividades de los modelos descritos

anteriormente en el capítulo 3. La tabla IV.XXIII presenta los resultados de la comparativa.

Tabla V.XXIII Relación entre el Modelo Propuesto y los Modelos Revisados.

Fases	Propuesta de Modelo Forense para un Servidor de Base de Datos	Modelos Propuestos por Instituciones Internacionales			
		DFRW	M. Abstracto	CFFTPM	M. Básico
Fase I	Preparación		X		
	Identificación del Problema	X	X		X
Fase II	Aseguramiento de la Escena				
	Inspección	X			
	Documentar la escena				
Fase III	Priorización de evidencia recogida	X	X		
	Recolección de Datos				
	Línea de tiempo			X	
Fase IV	Análisis de los medios				X
Fase V	Recuperación de Datos				
Fase VI	Preparación del Informe				X
	Organización de la Información				X
	Presentar el informe final	X	X		X

Fuente: Análisis práctico realizado en la Tesis

Elaborado por: Ana Juntamay y Nancy Macas

Fase I: Identificación

1. **Preparación.-** La fase de preparación ocurre antes de que se efectue la investigación como tal. Esto involucra un entendimiento inicial de la naturaleza del crimen y actividades, por ejemplo:

    a) Definir una serie de roles entre el personal involucrado con el objetivo de definir responsabilidades y generar un orden en todo el proceso.
    Ver Anexo 1:ROLES GENÉRICOS PROPUESTOS POR LA NIST

b) Preparación del equipo para empaquetado de fuentes de evidencia.
c) Realizar una evaluación de los recursos, alcance y objetivos necesarios para realizar la investigación interna.
d) La investigación debe respetar las diferentes imposiciónes legales y jurisdicciónales así como las restricciónes organizaciónales.
e) Es en esta etapa en donde se encuentran involucradas aquellas actividades como: órdenes de cateo, apoyo de la administración, autorizaciónes requeridas, etc. Se deben tomar en cuenta los derechos de privacidad de las partes relaciónadas con la investigación forense y, por lo tanto, se tendrá que presentar y entregar las notificaciónes legales pertinentes cuando sea necesario. En general, ciertos factores tales como: entrenamiento, educación, y experiencia de los investigadores deberán contribuir al éxito de esta fase. El contar con una minuciosa fase de preparación hará posible incrementar la calidad de la evidencia y minimizar los riesgos y amenazas asociados con la investigación. Como se puede ver, un objetivo importante de esta fase es la de desarrollar una estrategia apropiada para la investigación. Por lo cual es necesario tomar en cuenta la naturaleza del incidente y varios factores técnicos, legales y empresariales.

2. **Identificación del problema.-**Esta fase depende mucho de la parte afectada, la cual es la que debera descubrir la aparición o la ocurrrencia del incidente. Por lo tanto, esta etapa iniciará cuando el equipo de investigadores forenses reciba la notificación de que ha ocurrido un incidente que involucre el uso de un equipo servidor de base de datos SQL Server o MySQL.

   Parte de las acciónes iniciales involucrará la obtención de las características del evento:

   a) ¿Cuál es el problema?, ¿cuáles son las posibles afectaciónes?, si fuera posible obtener la información sobre las posibles causas etc., esta información servirá para crear un perfil sobre el estado inicial del evento el cual servirá para orientar las acciónes posteriores.

b) Identificar los dispositivos de almacenamiento o elementos informáticos que se consideren comprometidos y sean determinados como evidencia, su marca, modelo, caracteristicas, seriales, etc.
c) Identifique los posibles implicados o funciónarios que tengan relación con la investigación y efectue entrevistas con usuarios y admistradores responsables de los sistemas, documente todo y trate de lograr un conocimiento total de la investigación.

Fase II: Verificación

1. **Aseguramiento de la Escena.-** Esta fase se encarga principalmente de asegurar la escena del crimen para evitar accesos no autorizados y que la evidencia sea contaminada. A continuación se describe los pasos para asegurar la escena del crimen:
    a) Identificar la escena del delito, para ello se establecio un perímetro del lugar donde se encuentra el servidor de base de datos afectado.
    b) Para evitar daños posibles en la evidencia se procede a no manipular el equipo afectado
    c) Definir los sistemas involucrados en el incidente de seguridad
    d) Para garantizar la seguridad de la gente en la escena y la protección de la integridad de toda la evidencia. Los investigadores deben tener absoluto control de la escena y se debe evitar la posible intromisión de personas indeseadas; conforme el número de personas en la escena del crimen se encrementa, de igual forma las posibilidades de contaminación y de destrucción de la evidencia tambien aumentan.
    e) Preservar toda huella digital con el uso respectivo de guantes látex.
    f) Fotografiar el equipo vulnerado
    g) Los servidores deben dejarse en su estado actual hasta que se realice una evaluación apropiada. Si el servidor esta encendido, es mejor dejarlo encendido. De manera similar, si el servidor esta apagado, nunca se debe encender.
    h) Desconectar los cables de red
    i) Registrar la hora y fecha del sistema antes de ser apagado

j) De entre otras prioridades, la tarea de minimización de la corrupción o degradación de la evidencia se debe convertir en la mas sobresaliente. Cualquier objeto que pudiera convertirse en evidencia, no debe ser alterado para ello puede colocar etiquetas en las evidencias existentes

k) Tomar fotos de respaldo de las evidencias que han sido etiquetadas

2. **Inspección**.- Esta etapa implica identificar las fuentes potenciales de evidencia y formular un plan de busqueda apropiado. En un entorno con condiciónes complejas, esto podria no ser tan sencillo. En el caso de un servidor de base de datos, las principales fuentes de evidencia (despues del servidor de base de datos mismo) son: el adaptador de poder, el disco, cables , conexión de red, conexiona internet, etc.

   Debido a que la información presente en estos dispositivos puede ser facilmente sincronizada con computadoras, cualquier PC o computadora portatil en la escena del crimen tambien pudiera contener evidencia. Para determinar si se requiere la intervención de algun experto durante esta fase, se debe hacer una evaluación de los equipos en la escena. Es extremadamente importante identificar gente en la escena y conducir entrevistas preliminares. Los encargados de los servidores puden proporcionar información valiosa tal como: esquemas basicos de segutidad (contraseñas), nombres de usuarios, etc. Los investigadores deben tratar de obtener la mayor cantidad de información a partir de los diversas personas presentes en la escena o bien, relacionadas con el incidente. Si se requiere buscar elementos que no esten incluidos en la orden de cateo, se deben hecer los arreglos apropiados a la orden existente o bien, se debera obtener una nueva orden, la cual debera incluir los elementos adiciónales. Al final de la fase de inspección, debe ser desarrollado un plan inicial para la recolección y análisis de la evidencia

3. **Documentar la Escena.-** Esta parte involucra la correcta documentación de la escena del crimen mediante la toma de fotografias, esquematización y mapeo de la escena del incidente, se debe fotografiar todos los dispositivos electrónicos en la escena del crimen junto con los adaptadores de poder, cables, bases y otros

accesorios. Si el dispositivo movil esta encendido, entonces se debe documentar lo que aparece en la pantalla. Tambien se debe crear un registro de todos los datos visibles que se pueda revisar en cualquier momento y, que ayude a recrear la escena. Estos es paticularmente importante cuando un especialista forense tenga que presentar su testimonio en la corte, lo cual podria ocurrir varios mese despues de iniciada la investigación.

Fase III: Recolección de Evidencia

En esta fase se procede a recolectar la evidencia sin alterarla o dañarla, se autentica que la información de la evidencia sea igual a la original.

Se procederá hacer uso de las herramientas software ya definidas previamente, y asignar los equipos a las labores correspondientes.

Iniciar una Bitácora que nos permita documentar de manera precisa e identificar y autenticar los datos que se recogen de tipo:

- ¿Quién realizó la acción y porque lo hicieron?
- ¿Qué están tratando de lograr?
- ¿Cómo se realiza, incluidas las herramientas que se utilzará y los procedimientos que se siguieron?
- ¿Cuando se realizó la acción (fecha y hora) y los resultados?

1. **Priorización de Evidencia Recogida.** Las bases de datos contienen grandes almacenes de datos, para ayudar a grantizar la prioridad se asigna a las fuentes de datos un significado y un valor de volatilidad de entre 1-5, siendo 5 de mayor importancia y/o volatilidad.

   Los siguientes valores deberán ser utilizados en la fórmula siguiente para determinar la prioridad ***(10 –(número de significado) +(número de volatilidad)=prioridad(***. Utilizando la formula anterior, los datos almacenados relevantes serán priorizados como se muestra a continuación.

Tabla IV.XXIV Valores utilizados para determinar prioridad

Item	Importancia	Volatilidad	Prioridad
Sesiones & Conexiones SQL Server/MySQL	5	5	0
Logs de Transacción	5	4	1
Logs SQL Server/ MySQL	4	3	3
Archivos de Base de Datos SQL Server/MySQL	3	2	5
Logs de Eventos del Sistema	2	2	6

Fuente:http://www.blackhat.com/presentations/bh-usa-07/fowler/

Ahora que los almacenes de datos han sido identificados y priorizados, la recolección de datos puede tener lugar.

2. **Recolección de Datos.** Esta actividad 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. A medida que transcurre el tiempo en un incidente de seguridad, las pruebas pueden ser sobreescritas o dañadas. Para este caso particular se considerará que para descubrir un incidente en una base de datos de debe identificar los siguientes repositorios de evidencias:

Tabla IV.XXV Repositorios de Evidencias

SQL Server /MySQL	Sistema Operativo
o Datos volátiles de la base de datos o Datos de archivos de la base de datos o Archivos de Registro de base de datos o Plan de cache o Datos de la cache o Índices o Tempdb o Versión store	o Archivos de seguimiento Registros de suceso del sistema o Registros de error de SQL Server/MySQL o Página de Archivo o Memoria

Fuente:http://www.blackhat.com/presentations/bh-usa-07/fowler/

Realizar una copia imagen de los dispositivos(bit a bit), con una herramienta apropiada. Y firmar su contenido con un hash de MD5 o SHA1, generando asi el

segundo original, a partir de este se generaran las copias para el Análisis de datos, cada copia debe ser comprobada con firmas digitales nuevamente de MD5 o SHA1. Documente la evidencia con el documento de embalaje(y cadena de custodia) que puedan garantizar que se incluyen información acerca de sus configuraciónes.

3. **Cronología y Linea de Tiempo.** Esta actividad consite en construir una linea de tiempo incial que trazará los acontecimientos digitales notables que han sido identificados hasta la fecha y establecer un ámbito de la investigación que se utilizara durante esta fase de análisis.

   Se revisa los registros de errores de la base de datos obtenidos durante el paso de colección de evidencias con la fecha respectiva. Se añadirá a la linea de tiempo los eventos asociados con el proceso del servidor identificado (SPID) para el seguimiento de un determinado periodo de se sesiones dentro del servidor de base de datos. Los archivos de traza obtenidos durante el paso de recolección se importan a la estación de trabajo forense, donde se revisara los acontecimientos mas notables,y en base a los hechos identificados hasta el momento de la investigación,se procede a la construción de la linea de tiempo.

Fase IV: Análisis de Evidencia

1. **Análisis de Medios.** El cronograma establecido en la actividad anterior ahora se utilizará para establecer los limites en el análisis de medios.

   Se realizá un análisis de los registros de transacciones de la base de datos, seleccionando las columnas que contienen los datos mas relevantes basados en el alcance de la investigación.

   - Registro de Eventos de Windows (Windows event log)
     - Datos de Autenticación de SQL Server (fallas, inicio de sesión y desconexión satisfactorios)
     - Apagado y Encendido de SQL Server
     - Direccionamiento IP de conecciones de cliente de SQL Server
   - Registro de Errores (Error log)
     - Datos de Autenticación de SQL Server (fallas, inicio de sesión y desconexión satisfactorios)

    - Apagado y Encendido de SQL Server
    - Direccionamiento IP de conecciones de cliente de SQL Server
- Seguimiento Predeterminado de la Base de Datos(Default database trace)
    - Historial de autenticación completa
    - Operaciónes DLL (Esquema de cambios)
- Archivos Log y Archivos de Datos
    - Archivos adjuntos
    - Usar para obtener información de un esquema on-demand, contenido de pagina de datos,etc.
- Registro de Transacciónes Activas
    - Importación a Excel/ Acceso para revisión
    - Identificar sentecias DML y DDL
    - Mapa de transacciónes para un SPID
- Registro de Transacción – Operaciónes de Actualización
- La página DBCC recogerá la página modificada
- Revisión de la cabecera de la página detectará el objeto
- Recolectar el objeto esquema

A través del análisis, se habrá identificado toda la información relacionada con aquellos objetos considerados sobresalientes. De igual forma, se habría identificado cuáles son las características que presenten esos objetos. Al final de esta fase y por consecuencia, se deberá contar con una lista de características para cada pieza de información que resulte de interés.

Fase V: Recuperación de datos. En esta fase mediante la utilización de herramientas software se realizará la reparación y/o recuperación de la base de datos que se vio afectada por el incidente de seguridad o por algún error humano, que provocase la pérdida de registros, tablas y procedimientos.etc.

Fase VI: Preparación de informe

Consiste en documentar todas las acciones, eventos y hallazgos obtenidos durante el proceso forense. Todo el personal está involucrado en esta fase y es vital para asegurar la cadena de custodia de la evidencia. A continuación se muestra la estructura del informe:

1. **Organización de la información**
    - Recolectar toda la información generada en las fases anteriores e igual cualquier información anexa como notas o antecedentes.
    - Identifiquemos lo más importante y pertinente de nuestra investigación
    - Emitir conclusiones

2. **Presentar el Informe Final**

    Debe ser claro, conciso y escrito en un lenguaje entendible para gente común (no tan técnico). Debe contener como mínimo:

    - Objetivo del Informe
    - Autor del Informe
    - Resumen de Incidentes
    - Pruebas
    - Detalles
    - Conclusión
    - Documentos de Respaldo

    Tabla de Contenidos del Informe

    1. Análisis Preliminar
    2. Cronograma de Actividades
    3. Proceso de Análisis y entorno de investigación
    4. Aplicación de la guía de procedimientos
    4. Conclusiones
    5. Anexos

    Descripción de parámetros del Informe

    1. Análisis Preliminar

    Se explica sobre la finalidad del documento, definiendolo como el informe técnico en respuesta a un proceso de análisis forense.Es importante indicar:

Portada

- Identificación en forma rápida del contenido del informe, es decir detallar claramente el objetivo del mismo, dando a conocer en que se centro el análisis, es decir un resumen del caso a resolver.
- Quien solicito el analisis forense, donde se realizo, fecha del informe.

Información de los peritos o grupo de investigación.

- Nombres
- Números de cédulas
- Números de Licencia Profesional

Antecedentes

- Descripción detallada de los equipos intervenidos
- Especificar características de los equipos
- Listar los nombres de las herramientas utilizadas y su función

2. Cronograma de Actividades

Secuencia de acciones por parte de los peritos informáticos en determinar tiempos, se pueden ayudar con software como el Project de Microsoft office para su estructuración.

3. Proceso de análisis y entorno de investigación

El propósito este capítulo es detallar las herramientas empleadas en el análisis así como la construcción del entorno de análisis forense usado para la investigación.

Se detalla la secuencia a de actividades llevada a cabo para la obtención de las evidencias y el análisis de las mismas.

En otras palabras involucra las fases de la guía de procedimientos

4. Conclusiones

Finalmente este apartado agrupa los principales puntos que se obtienen como consecuencia del análisis forense efectuado

5. Anexos

Pueden ser formularios, reglamentos, entrevistas, tablas, etc. utilizadas para realizar los pasos anteriormente expuestos.

CAPÍTULO VI

APLICACIÓN DE LA GUIA DE PROCEDIMIENTOS DE ANÁLISIS FORENSE EXPUESTOS EN DESITEL-ESPOCH

6.1. INTRODUCCIÓN

Es necesario comprender la importancia de aplicar en forma adecuada cada una de las fases que se incluye en la guía de procedimientos, para la cual se cita a continuación cada una de ellas aplicadas en un escenario real que se detalla a continuación.

6.2. LIMITACIÓNES PARA LA APLICACIÓN DE LA GUÍA

La guía presenta las siguientes limitaciones:

- El alcance de la guía está limitada a servidores de base de datos SQL Server 2005 y MySQL 5.x, esto se deriva a que estas bases de datos son utilizadas en los sistemas más representativos de gestión Académica y Administrativa en la ESPOCH.
- La guía no se aplicará en todo los casos, ya que se debe tener en cuenta la gravedad del incidente y si es justificable o no la aplicación de la guía de procedimientos, puesto que involucraría mucho tiempo y costos. Por ejemplo si un Docente manifiesta que no modifico la nota de un estudiante, este evento

puede ser resuelto por el módulo de auditoría del sistema Académico, pero si no es parte de los procesos del modulo se aplicaría la guía propuesta.

Procesos del Modulo de Auditoria del Sistema Académico de la ESPOCH (OASIS)

- Ingreso de Notas
- Control y Autenticación de Usuarios
- ¿Quién Matriculó?, ¿Quién generó la Matricula?
- Fallos de Ingreso al Sistema (si hay 3 intentos fallidos se bloquea la cuenta)

6.3. CONDICIONES MÍNIMAS PARA LA APLICACIÓN DE LA GUÍA

La guía presenta las siguientes Condiciones:

- En general para que la guía de análisis forense pueda ser aplicada, se requiere que el host sobre el que está el servidor de base de datos posea conectividad de red entre la victima (servidor afectado) y la estación forense, esto implica que todos los servicios de red TCP/IP, así como los equipos activos de red del Backbone institucional estén funcionando correctamente en el segmento de red entre estos dos equipos.

6.4. REALIZACIÓN DE LOS ESCENARIOS DE ATAQUE

Para llevar a cabo los escenarios de ataque se deben tener en consideración los siguientes elementos iníciales:

- Estación de Trabajo Forense.
- Servidor de base de datos SQL SERVER 2005(BD de Sistema Académico OASIS).
- Equipo de Ataque

A continuación se presenta una descripción de los elementos iníciales que se utilizarán para los escenarios planteados:

6.5. HARDWARE Y SOFTWARE DE LOS ESCENARIOS DE ATAQUE

Tabla IV.XXVI Estación Forense

HARDWARE	SOFTWARE
• Computador portátil HP Pavilon DV6120 • Procesador Intel Pentium 4 CPU 2.40GHz • Memoria RAM 4GB • Disco Duro - Capacidad 320 GB	• **Sistema Operativo:** Microsoft Windows XP • **Programas:** – Mozilla Firefox 4.0 – Reproductor de Windows Media 11 – VMware Workstation

Tabla IV.XXVII Servidor de Base de Datos SQL Server 2005

HARDWARE	SOFTWARE
• Computador Personal D865GVHZ • Procesador Intel Core2 Duo 2.0GHz • Memoria RAM 1.0 GB • Disco Duro - Capacidad 20 GB	• **Sistema Operativo:** Microsoft Windows Server 2003 SP 2 • **Programas:** – Microsoft .NET Framework 3.5 – Windows Internet Explorer 8 – Microsoft SQL Server 2005

Tabla IV.XXVIII Descripción del Sistema

Nombre del Servidor:	WEBSERVE-240D78\SQL2005
Sistema Operativo	Microsoft Windows Server 2003 SP 2
Database Versión:	9.0
Dirección IP:	172.30.60.5
Modo de Autenticación	Autenticación SQL Server

Tabla IV.XXIX Esquema de la Base de Datos a atacar

Nombre de la base de datos:	OAS_Sistemas
Número de tablas	87
Número de procedimientos almacenados	154
Número de Vistas	24
Número de Funciones	43
Tipos de Datos Definidos por el Usuario	39

Tabla IV.XXX Equipo de Ataque

HARDWARE	SOFTWARE
• Procesador Intel Pentium 4 CPU 2.40GHz • Memoria RAM 512 MB • Disco Duro - Capacidad 80 GB	• **Sistema Operativo:** Microsoft Windows XP Professional SP 3.0 • Reproductor de Windows Media

Para la realización de los escenarios se clonó el sitio web académico de la ESPOCH OASIS con la Herramienta Internet Download Manager 6.06. Ver Anexo 2.

6.5.1. ESCENARIO 1

6.5.1.1. SQL Injection

En este escenario se va a utilizar los siguientes elementos:

- Dos computadoras, una que tenga instalado SQL Server 2005, la misma que tendrá la copia de la Base de Datos del Sistema Académico y el sitio web clonado y que sea vulnerable a la inyección SQL. Mientras que la segunda máquina será el atacante y debe tener acceso al sitio web de la víctima.
- Un computador portátil que será la estación forense.

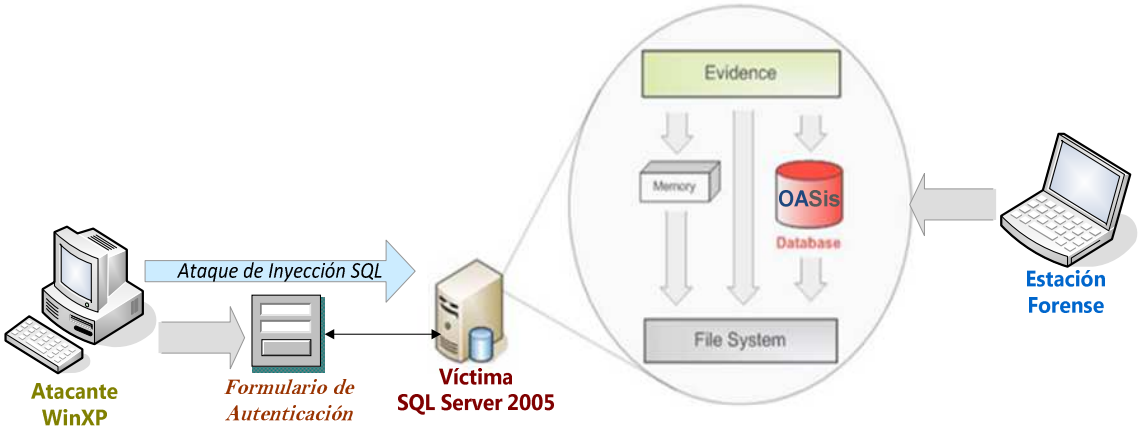


Figura VI.112. Arquitectura del escenario ataque Inyección SQL

La máquina victima está conectada a la red de la ESPOCH y posee una dirección IP dinámica como se muestra en la siguiente figura.

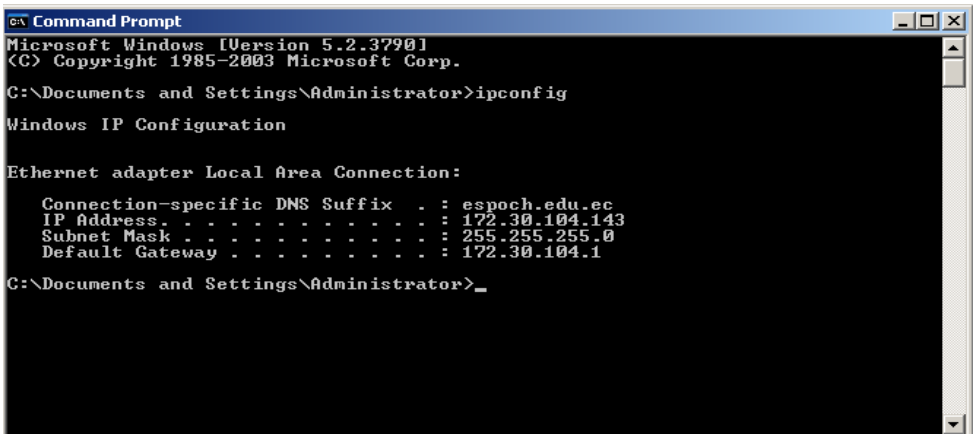


Figura VI.113. Dirección IP de la máquina Victima

El atacante ingresa al sitio web para poder autenticarse y proceder a realizar la inyección SQL.

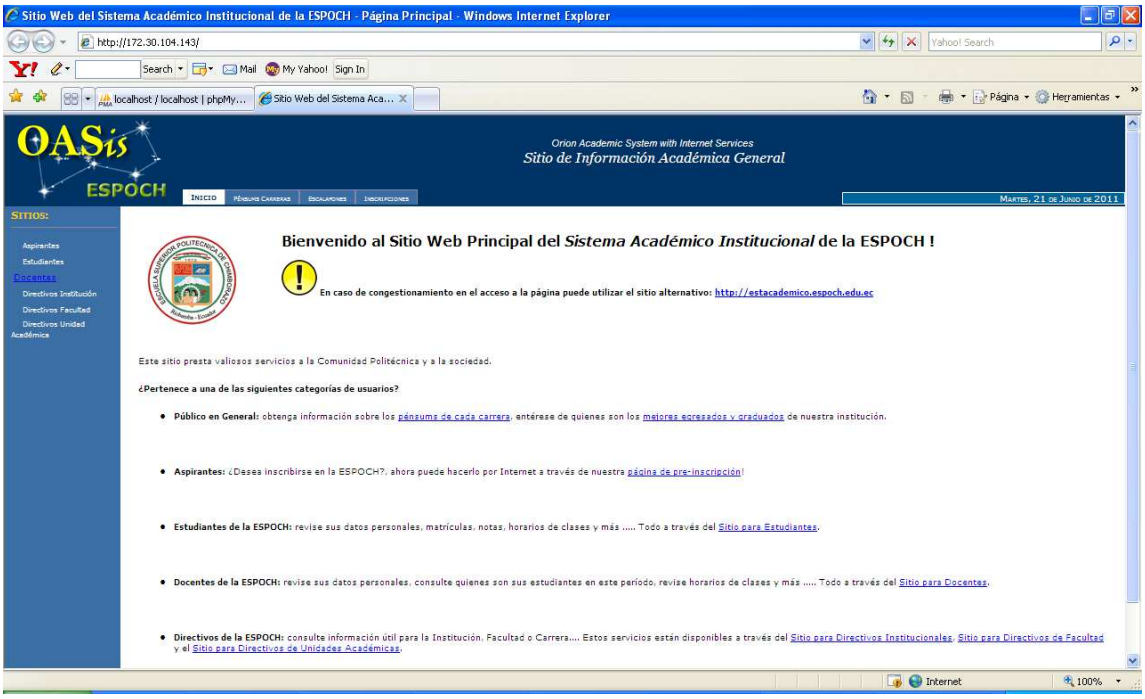


Figura VI.114. Página principal del Sitio web Académico de la ESPOCH

Luego el atacante ingresar a la página de autenticación donde va a ingresar el código malicioso para llevara a cabo la inyección SQL.

La inyección SQL ejecutada es: ususario: 'or 1=1—y password: *.

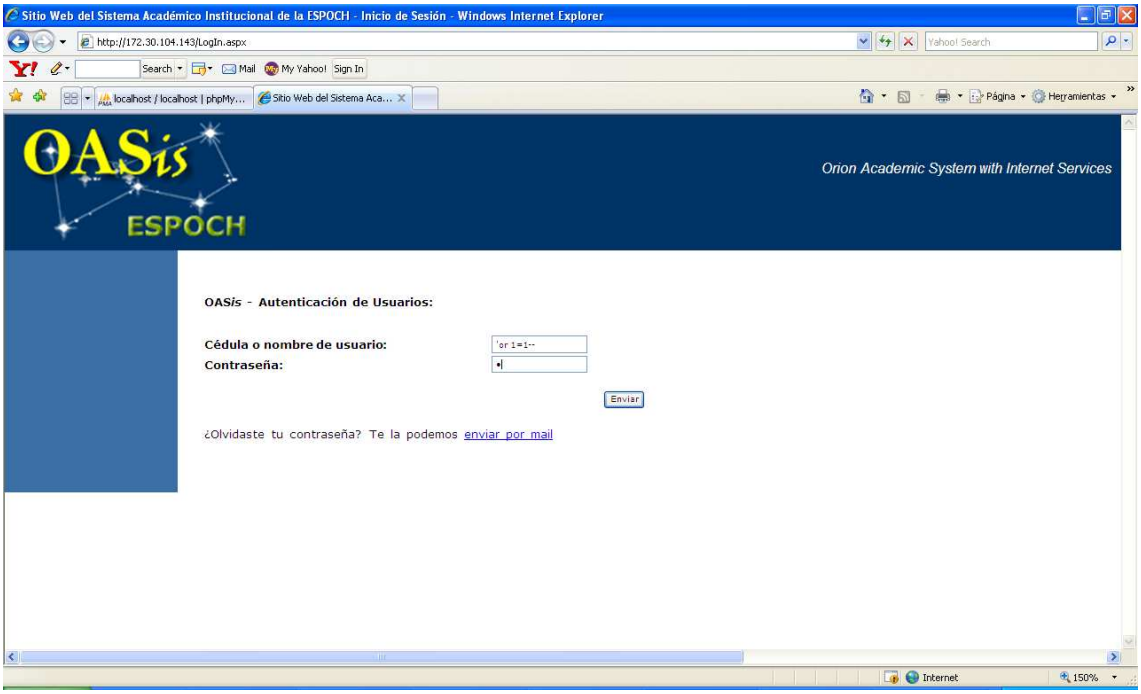


Figura VI.115. Ingreso de código para ejecutar inyección SQL.

Una vez ejecutada la inyección SQL el atacante ingresa al sitio web de acuerdo al tipo de usuario (docente, estudiante, directivo) previamente selecciónado.

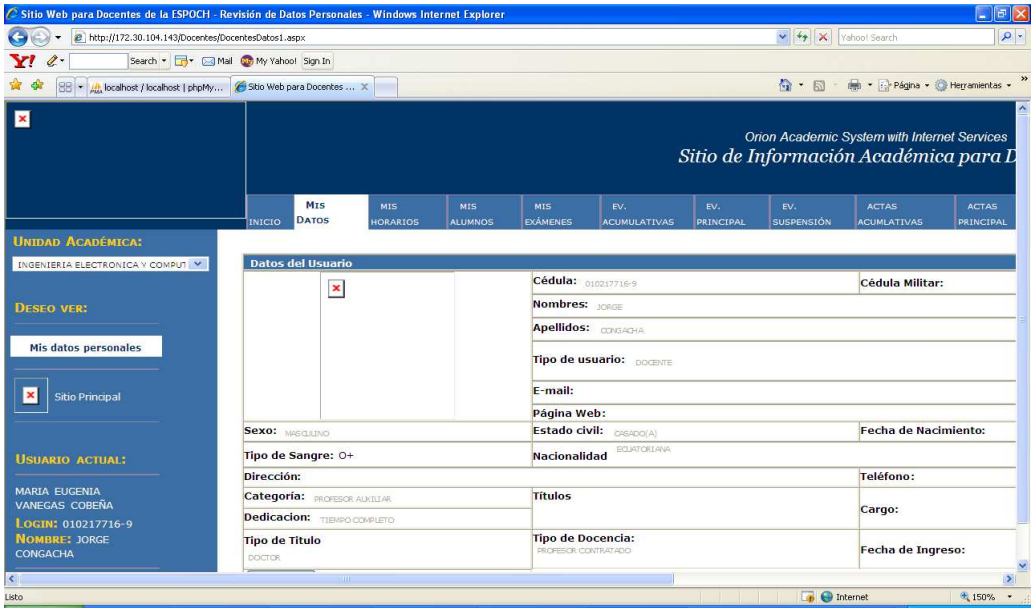


Figura VI.116. Página principal de Docente

6.5.2. ESCENARIO 2

6.5.2.1. Ataque de fuerza bruta con Dicciónario

- El atacante tiene como sistema operativo la distribución de Linux orientada a seguridad Backtrack la cual se encuentra disponible en su última versión en http://www.remote-exploit.org/backtrack.html
- Archivo .txt que sea el diccionario para el ataque de fuerza bruta.

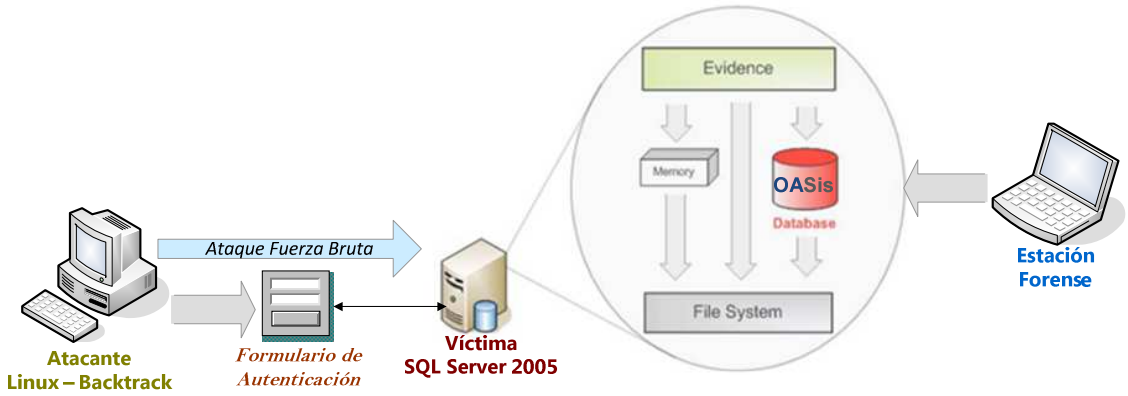


Figura VI.117. Arquitectura del escenario ataque Fuerza bruta con Diccionario

El primer paso del ataque consiste en comprobar si hay conexión entre la máquina víctima y el atacante.

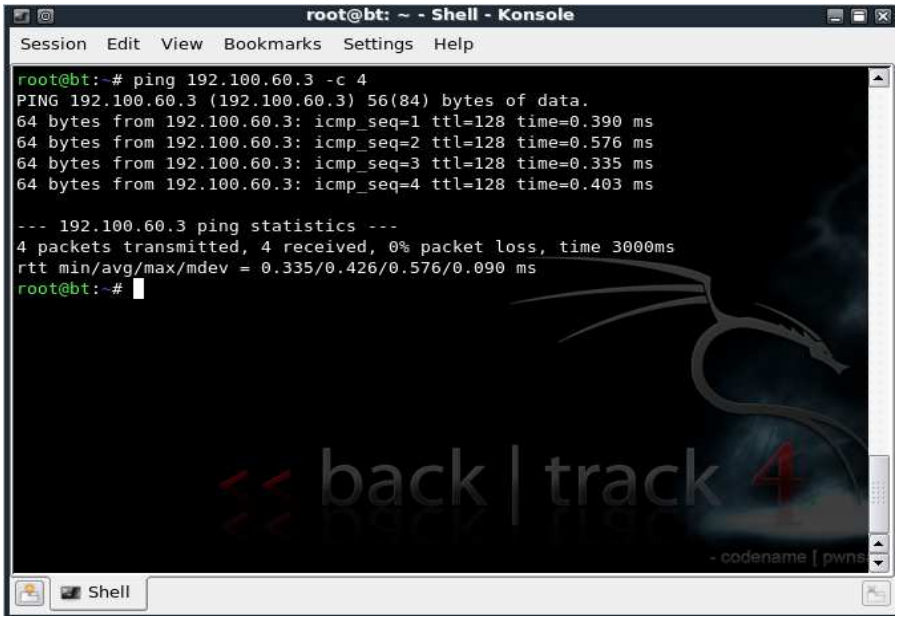


Figura VI.118. Conexión entre máquina víctima y atacante

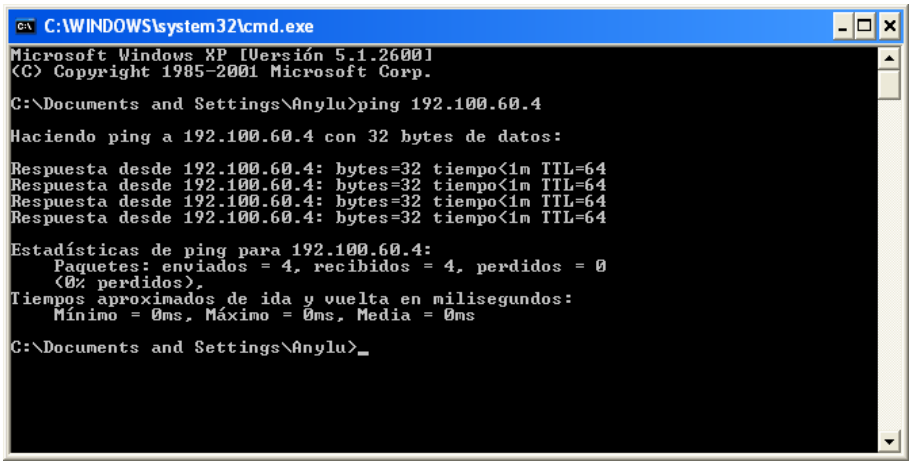


Figura VI.119. Conexión correcta entre máquina víctima y atacante

Se utiliza la herramienta zenmap para ver el puerto que utiliza SQL Server 2005

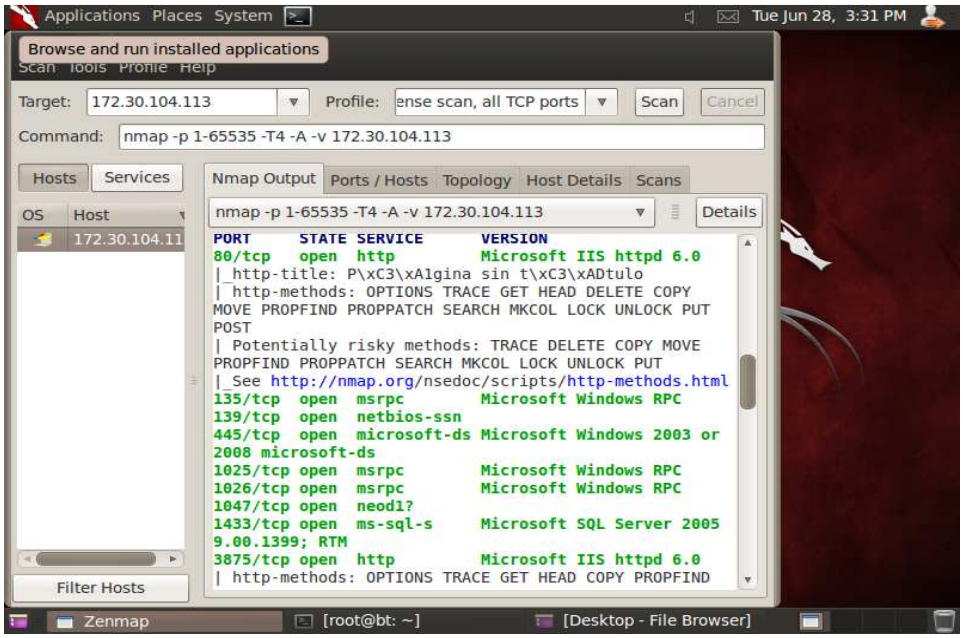


Figura VI.120. Herramienta Zenmap

El ataque se realiza desde el sistema operativo Backtrack 5.0 que contiene una herramienta para ataque de fuerza bruta con diccionario denominada Medusa. Además se tiene un archivo de texto denominado claves.txt que se utilizará para este escenario.

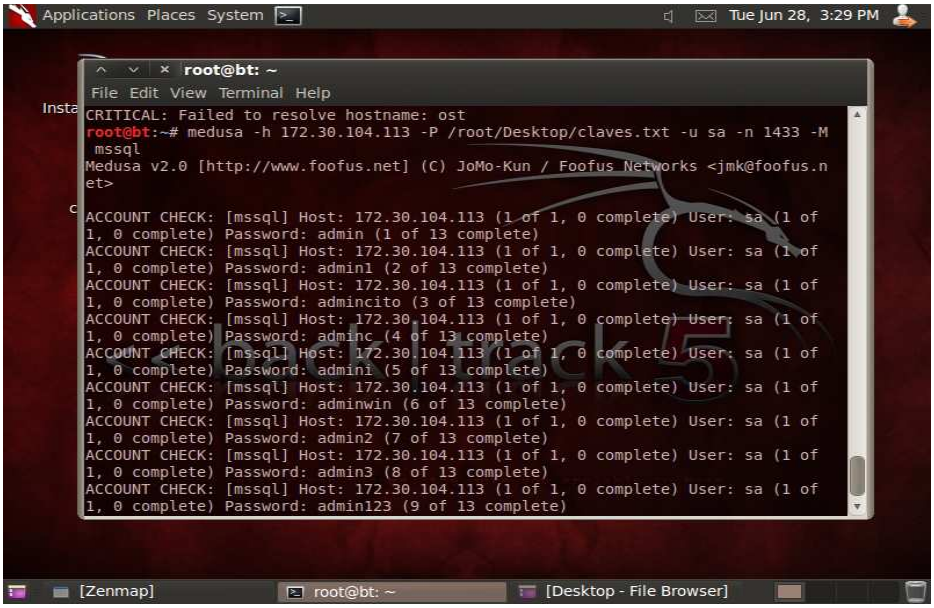


Figura VI.121. Ataque de fuerza bruta con diccionario

Ahora que se conoce el password para acceder al Servidor SQL Server 2005 se inicia sesión con SQL Server Management Studio.

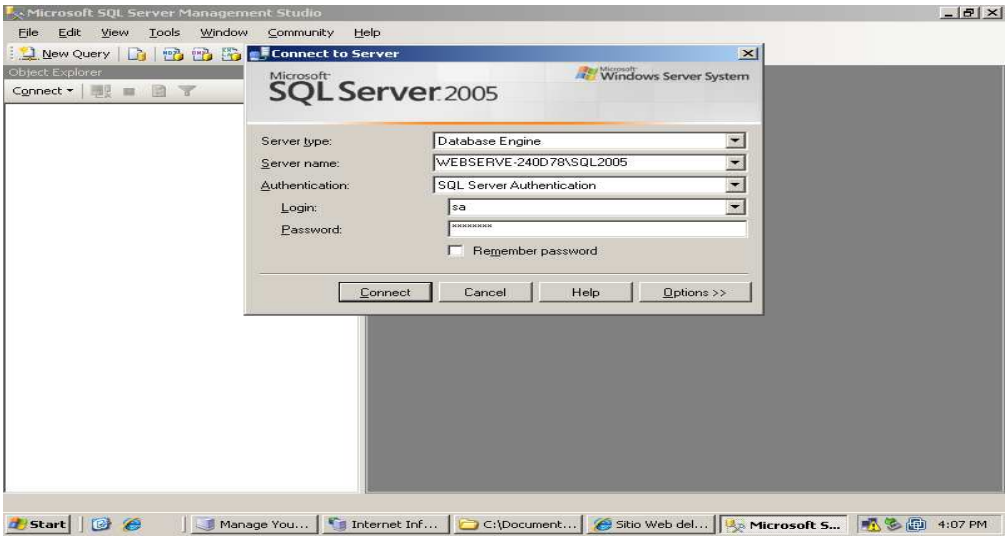


Figura VI.122. Ingreso a SQL Server después de ataque.

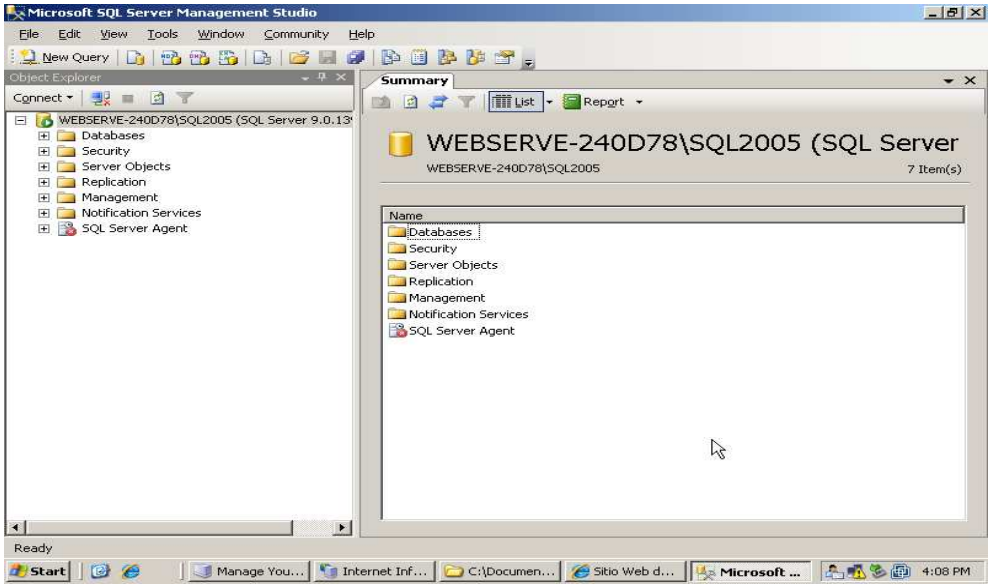


Figura VI.123. Visualización de contenido del servidor

6.5.3. ESCENARIO 3

6.5.3.1. Ataque a las cuentas de usuario

Ingresar a Microsoft SQL Server 2005 mediante la herramienta SQL Server Management Studio.

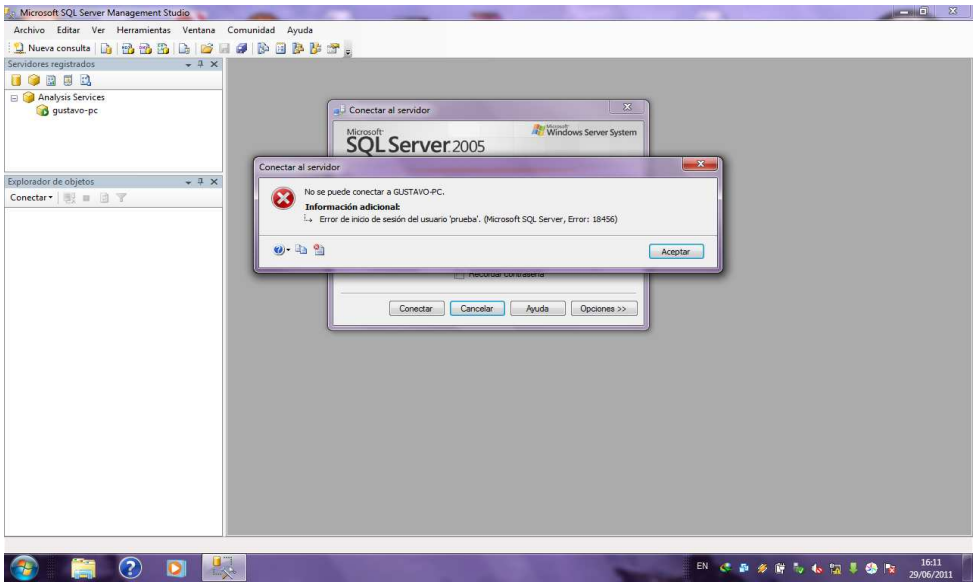


Figura VI.124. Error de inicio de sesión

Abrir el programa Advanced SQL Password Recovery

Figura VI.125. Pantalla principal de Advanced SQL Password Recovery

Antes de utilizar esta herramienta proceder a bajar los servicios de SQL

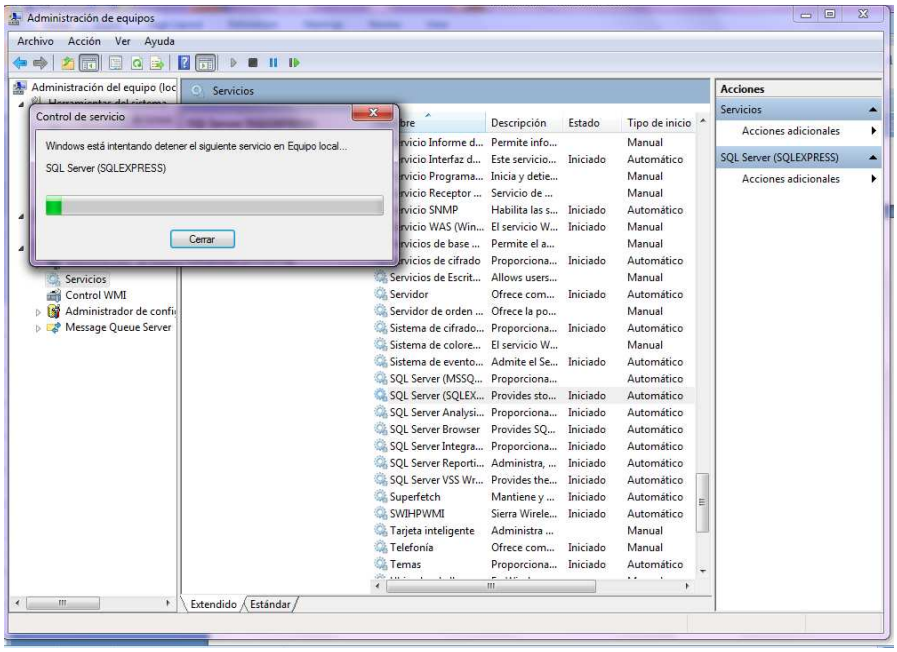


Figura VI.126. Servicio de SQL SERVER detenido.

Dar click en Open File para ingresar al archivo master.mdf

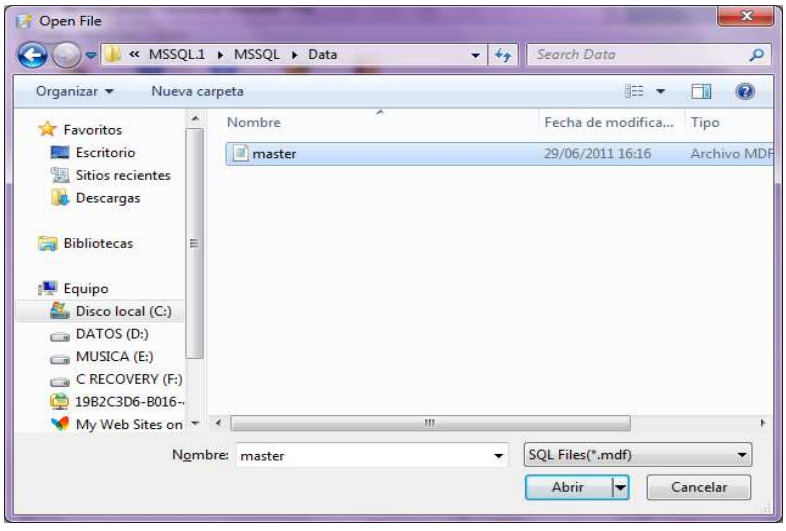


Figura VI.127. Archivo .mdf.

Esperar que el programa encuentre los usuarios de la base de datos

Seleccionar el usuario al cual se le va a cambiar el password

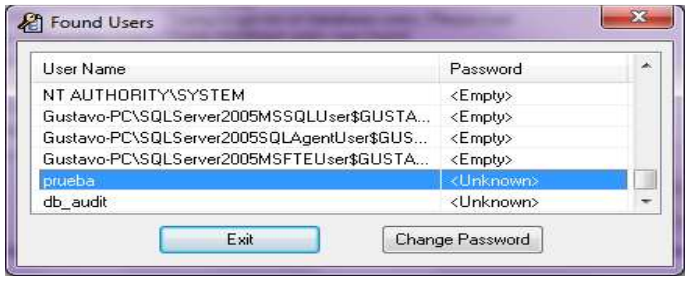


Figura VI.128. Usuarios SQL encontrados.

Ingresar el nuevo password

Figura VI.129. Ventana Set Password.

Verificar que el password se cambie correctamente

Dar click en exit, para observar el estado del programa.

Figura VI.130. Ventana Estado de Advanced SQL.

Ingresar a Microsoft SQL Server con el nuevo password

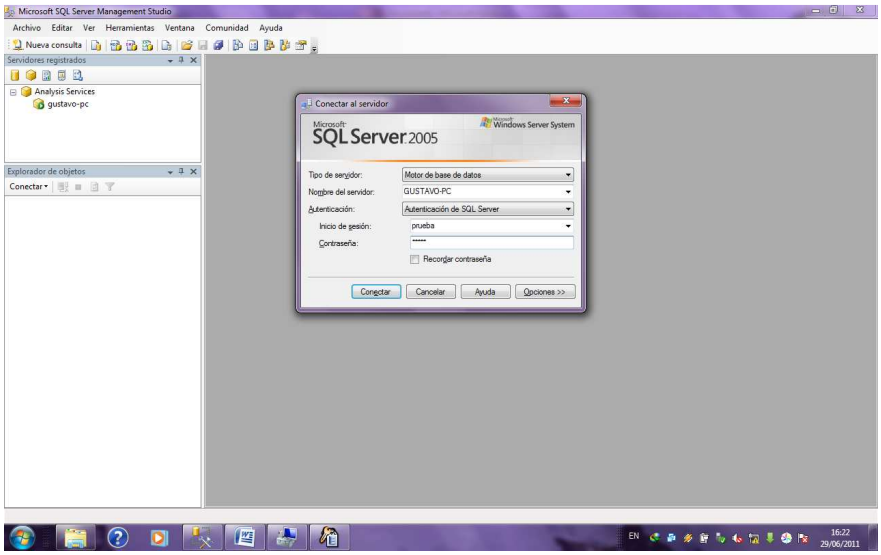


Figura VI.131. Ingreso a SQL Server con el nuevo password.

Observar que el servidor se conecta con el nuevo password e ingresar a la base de datos, esta herramienta es útil debido a que si se olvida la contraseña se puede cambiar y de esta forma no perder la información pero también esta herramienta permite hackear la base de datos ya que permite el cambio de password sin ninguna restricción.

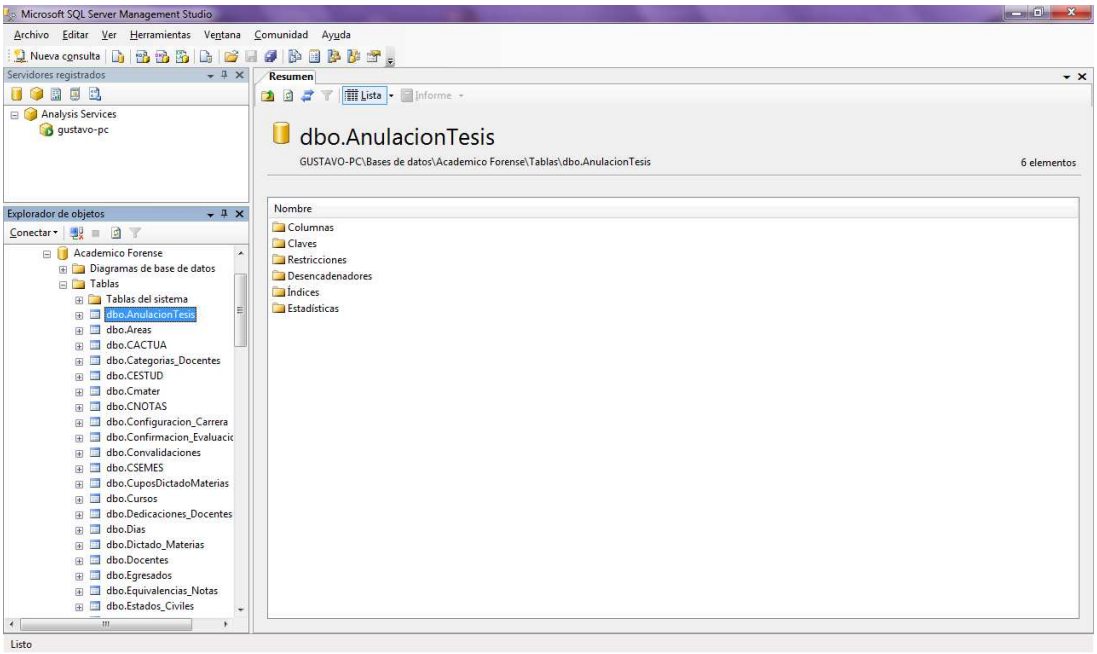


Figura VI.132. Visualización del contenido del servidor.

6.5.4. ESCENARIO 4

6.5.4.1. Errores Humanos

Errores del Administrador del Sistema

En caso de que el Administrador de la Base de Datos elimino accidentalmente registros de la Base de Datos.

El DBA elimina 3 registros de la tabla Parametros_Carrera, a continuación se muestra la tabla antes de ser eliminada los registros.

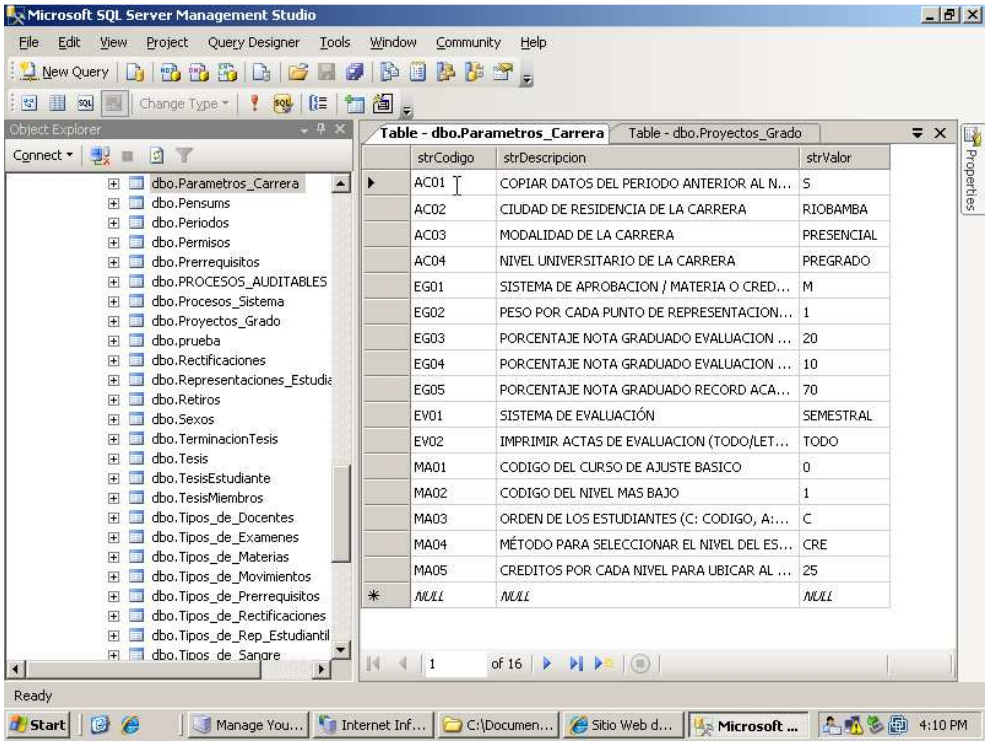


Figura VI.133. Tabla antes de ser eliminada los registros.

En esta figura se ve la tabla sin 3 registros.

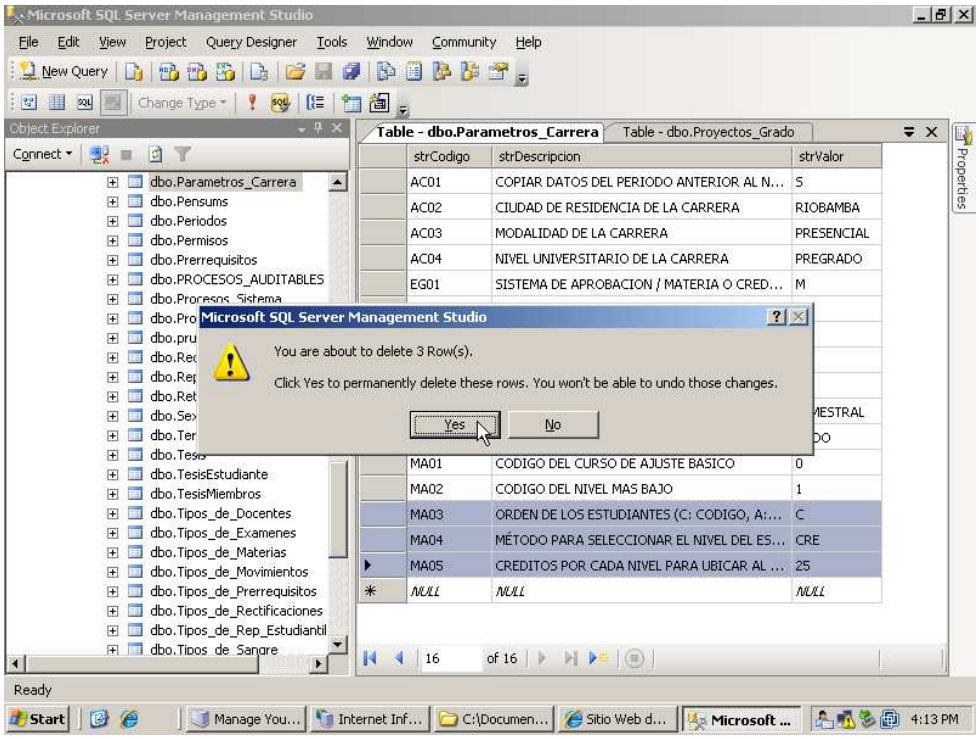


Figura VI.134. Eliminación de registros

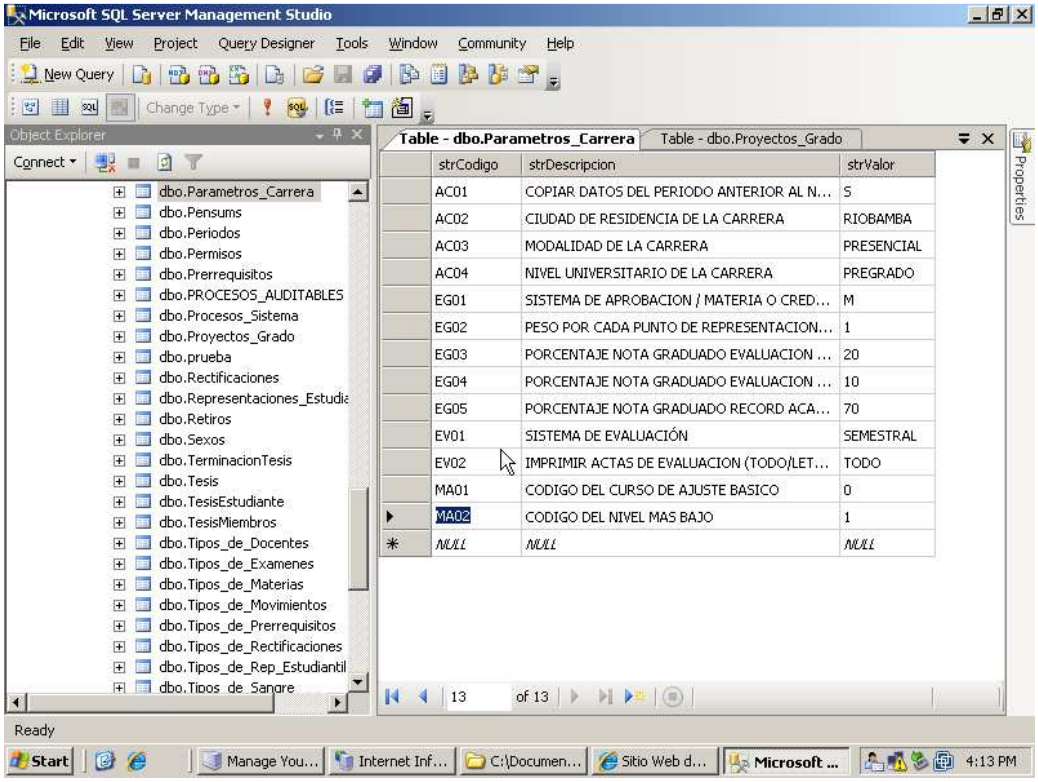


Figura VI.135. Tabla después de ser eliminada los registros.

Errores humanos del usuario final

Se tiene los siguientes datos en la base de datos antes de ser modificado por la Docente Lorena Aguirre.

Ahora ingresa al sitio web y modifica sus datos.

Figura VI.136. Pantalla principal del Sistema OASis

Página home del Docente

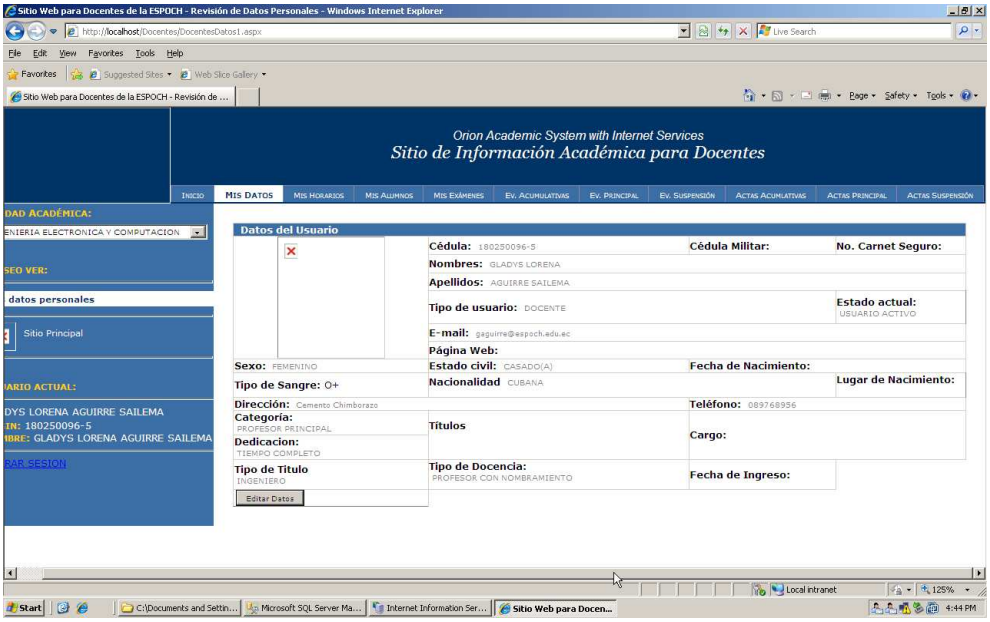


Figura VI.137. Pantalla de Datos del Docente.

Luego de guarda los datos

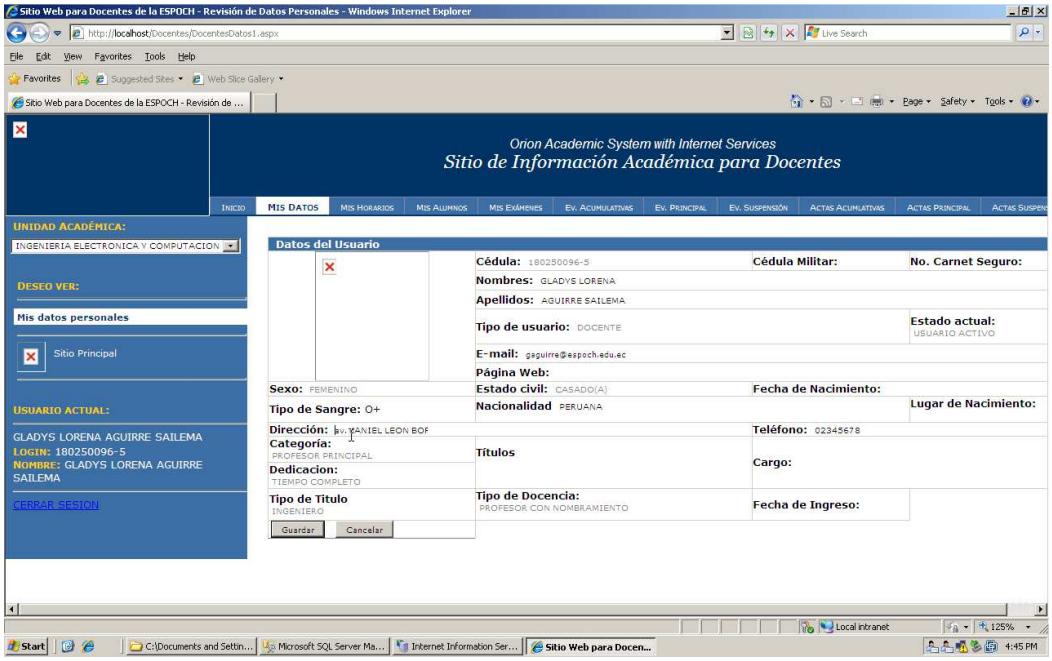


Figura VI.138. Datos modificados del Docente.

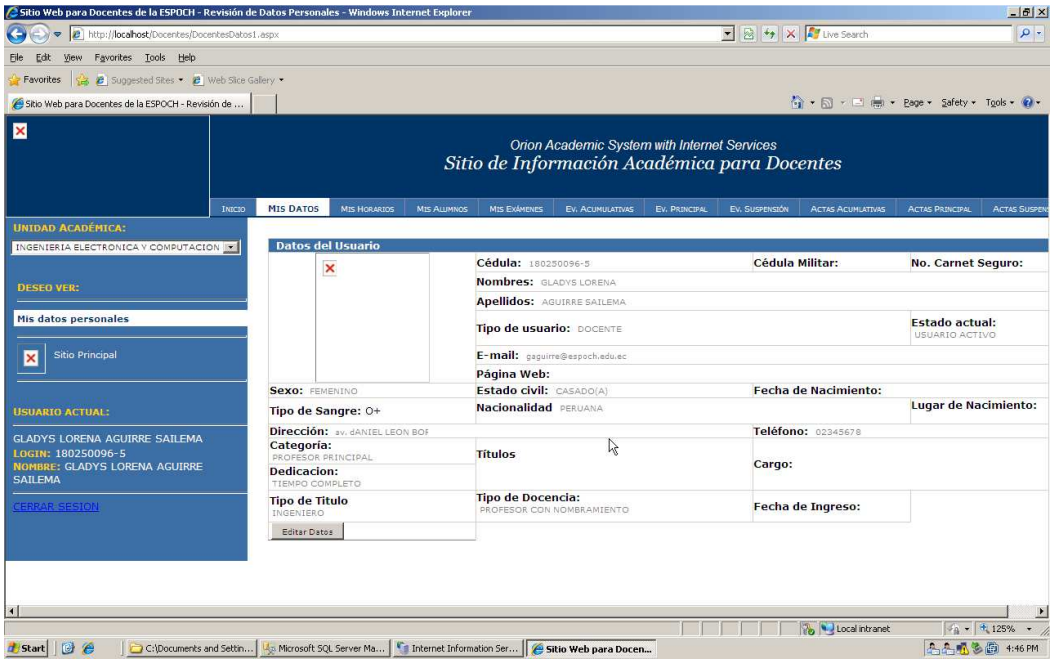


Figura VI.139. Datos guardados del Docente.

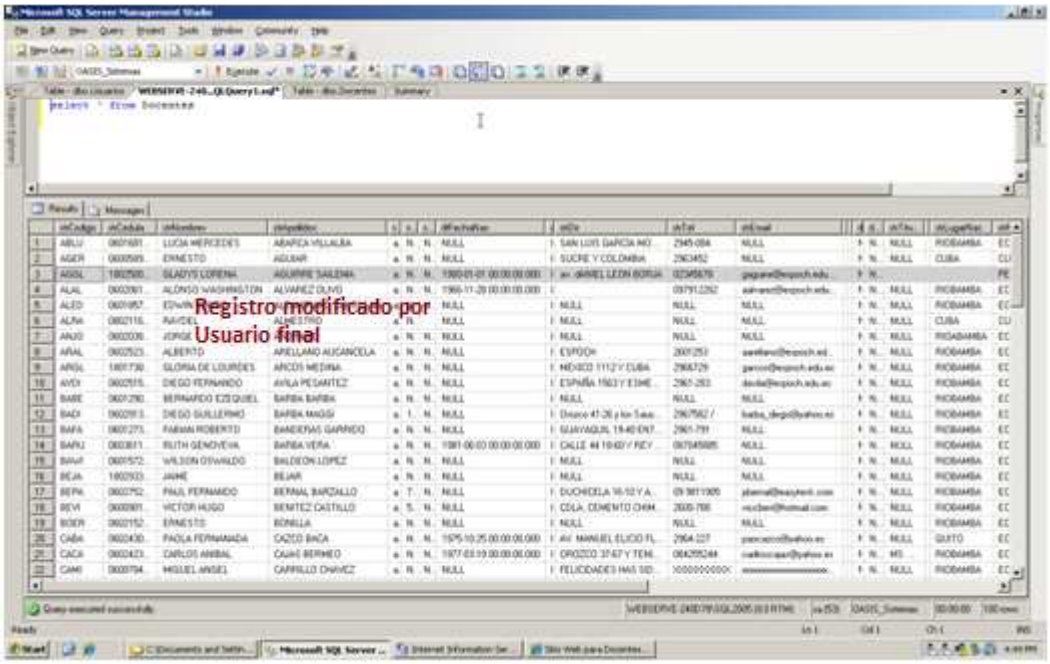


Figura VI.140. Registro modificado por el usuario final

6.6. DESCRIPCIÓN DEL CASO DESITEL – ESPOCH

El proceso de análisis forense informático inicia ante la solicitud realizada por el Director del Departamento de Sistemas y Telemática (DESITEL) de la ESPOCH, el caso se enmarca en analizar la copia de la base de datos académico aplicando la guía de procedimientos de análisis forense propuesta, para no comprometer el equipo sospechoso y recolectar evidencias.

El quipo de investigación se ha conformado de la siguiente manera: 2 investigadores Ana Juntamay portadora de la cédula de identidad 0604230219 y Nancy Macas portadora de la cédula de identidad 0604008706. Se acepto con acuerdo entre las partes involucradas, siendo las mismas responsables de la Institución y el equipo de investigación.

Se requiere conocer información sobre la Base de Datos Académico.

6.7. PROCESO APLICATIVO DE ANALISIS FORENSE CONJUNTAMENTE CON LA GUÍA DE PROCEDIMIENTOS Y HERRAMIENTAS

INFORME PERICIAL

6.7.1. ANALISIS PRELIMINAR

- **Breve Identificación del Contenido**

  El proceso de análisis forense informático inicia ante la solicitud realizada por el Director de DESITEL, el caso se enmarca en la detección de vulnerabilidades y recuperación de base de datos importante para la institución que fue alterada y conocer registros de la acción hora, fecha, cuenta de usuario, cabe mencionar que la base de datos pueden ser modificada o eliminada ya sea por personal interno o externo a la institución.

  Se ha trabajado haciendo uso de diversas herramientas para no comprometer el equipo sospechoso y recolectar evidencias.

- **Análisis forense solicitado por:**

  Dr. Carlos Buenaño

  DIRECTOR DE DESITEL

- **Donde se realizo:**

  Departamento de Sistemas y Telemática (DESITEL) de la ESPOCH

- **Fecha del Informe:**

  22 de Junio de 2011

- **Información de los Peritos o Grupo de investigación**

Nombres	Número de cédula	Número de licencia profesional
Ana Juntamay	0604230219	AJ4015
Nancy Macas	0604008706	NM3252

- **Antecedentes**

  Descripción detallada de los equipos intervenidos:

  Nombre del equipo: WEBSERVER-240d78

  Sistema operativo: Microsoft Server 2003 SP2

Especificar características de los equipos

Memoria RAM: 1 GB

Capacidad de disco duro: 20GB

Lista de los nombres de las herramientas utilizadas y su función

Las herramientas que se utilizaron son las siguientes:

- SQL Server Management Studio Express
- Microsoft Forensic Tooolchest
- SQLCMD
- MD5SUM

6.7.2. CRONOGRAMA DE ACTIVIDADES DEL INFORME DE ANÁLISIS FORENSE

		Nombre de tarea	Duración	Comienzo	Fin	Pre
1		**IDENTIFICACIÓN**	**1 día?**	**lun 20/06/11**	**lun 20/06/11**	
2		Preparación	1 día?	lun 20/06/11	lun 20/06/11	
3		Identificación del Problema	1 día?	lun 20/06/11	lun 20/06/11	
4		**VERIFICACIÓN**	**3 días?**	**mar 21/06/11**	**jue 23/06/11**	
5		Aseguramiento de la escena	1 día?	mar 21/06/11	mar 21/06/11	
6		Inspección	1 día?	mié 22/06/11	mié 22/06/11	
7		Documentar la Escena	1 día?	jue 23/06/11	jue 23/06/11	
8		**RECOLECCIÓN DE LA EVIDENCIA**	**3 días?**	**vie 24/06/11**	**mar 28/06/11**	
9		Recoleccion de Datos	1 día?	vie 24/06/11	vie 24/06/11	
10		Priorización de Evidencia Recogida	1 día?	lun 27/06/11	lun 27/06/11	9
11		Cronoología y Linea de Tiempo	1 día?	mar 28/06/11	mar 28/06/11	10
12		**ANALISIS DE EVIDENCIA**	**2 días?**	**mié 29/06/11**	**jue 30/06/11**	
13		Analisis de Medios	1 día?	mié 29/06/11	mié 29/06/11	
14		Analisis con Hermientas Forenses	1 día?	jue 30/06/11	jue 30/06/11	13
15		**RECUPERACIÓN DE DATOS**	1 día?	vie 01/07/11	vie 01/07/11	
16		**PREPARACION DEL INFORME**	3 días?	lun 04/07/11	mié 06/07/11	15

Figura VI.141. Cronograma de Actividades del informe de Análisis Forense

6.7.3. PROCESO DE ANÁLISIS Y ENTORNO DE INVESTIGACIÓN

Una vez sucedido el incidente de seguridad, el técnico o usuario comunicara al Director persona que represente al Departamento de Sistemas y Telemática (DESITEL)quien inmediatamente emitirá una circular en la que se restringe el acceso al Servidor de BD

Académico (Ver Anexo 3), luego se enviará un oficio que autorice el proceso de análisis forense (Ver Anexo 4).

El proceso a realizar para aplicar la guía de procedimientos con sus respectivas fases se describe mediante el uso de Diagramas de Caso de Uso que puede ver en el Anexo 5.

GUÍA DE PROCEDIMIENTOS

FASE I: Identificación

1. Preparación

a) Se definió roles de acuerdo al Organigrama del Departamento de Sistemas y Telemática(DESITEL) de la ESPOCH. Ver Anexo 6.

b) El Director de DESITEL emitio un oficio para designar una persona que acompoñe a la persona o grupo de investigadores forenses.Ver Anexo 7.

c) Se realizó una evaluación de los recursos, alcance y objetivos necesarios para realizar la investigación interna.

d) Se revisó el reglamento del Departamento de Sistemas y Telematica (DESITEL). Ver Anexo 8.

e) Se aplicó formulario de orden de cateo Ver Anexo9.

2. Identificación del problema

a) Se determino cual es el problema, afectaciónes y las posibles causas:

PROBLEMA	Alguien ingresa al Servidor de Base de datos y altero la información almacenada en la Base de Datos OAS_Sistemas.
AFECTACIÓNES	Se alterna información confidencial que afecta la integridad y veracidad de esta.
POSIBLES CAUSAS	Por un error humano la momento de ingresar la información al sitio web o alguien que desea ingresar información alterada.

b) Se identifico los dispositivos de almacenamiento o elementos informáticos que se consideraron comprometidos y fueron determinados como evidencia, su marca, modelo, caracteristicas, seriales, etc.Ver Anexo 10.
c) Lista de los posibles implicados o funciónarios que tuvieron relación con la investigación, usuarios y admistradores responsables del Sistema, Ver Anexo 11

Fase II: Verificación

1. **Aseguramiento de la escena.-**Para realizar la siguiente actividad se seguiran los siguientes pasos:

a) Se identifico la escena del delito, para ello se establecio un perímetro del lugar donde se encuentra el servidor de base de datos afectado.
b) Se evito daños posibles en la evidencia (no manipular el equipo afectado).
c) Se definio los sistemas involucrados:
Windows Server 2003 SP2
d) Se permitio el acceso solo de personas involucradas en el análisis de la evidencias.
e) Se preservo toda huella digital con el uso respectivo de guantes látex.
f) Se fotografio el equipo vulnerado
g) Se reviso el estado de los equipos para poder identificar las evidencias volátiles.
h) Se desconecto los cables de red
i) Se registro la hora y fecha del sistema antes de ser apagado
j) Se coloco etiquetas en las evidencias existentes
k) Se tomo fotos de respaldo de las evidencias que han sido etiquetadas

2. **Inspección**

- Formulario de Resultado de Evidencias y Formulario de Estado de Evidencias ver anexo 11 Y 12.
- Se identifico las fuentes potenciales de evidencia, en el caso de un servidor de base de datos, las principales fuentes de evidencia en el Servidor de Base de Datos son los repositorios.

- Se identificó la gente en la escena y se condujó entrevistas preliminares. Los encargados de los servidores puden proporciónar información valiosa tal como: esquemas basicos de seguridad(contraseñas), nombres de usuarios, etc.

3. Documentar la escena

Se reunió toda la información recolectada como fotografías de todos los dispositivos electrónicos en la escena del crimen junto con los adaptadores de poder, cables, bases y otros accesorios. Ver Anexo 13.

Fase III: Recolección de Evidencia

- ¿Quién realizó la acción y porque lo hicieron?
  El Examinador Forense (Nancy Macas) para mantener la confiabilidad de la evidencias.
- ¿Qué están tratando de lograr?
  Mantener la cadena de custodia
- ¿Cuando se realizo la acción (fecha y hora) y los resultados?
  Hora Sistema: 09:30 am
  Fecha Sistema: 15 de Enero del 2009
  Hora Actual: 09:32
  Fecha Actual: 15 de Enero del 2009

Priorización de Evidencia recogida

Se priorizo la evidencia de acuerdo a la tabla de valores utilizados para determinar prioridad, una vez los datos han sido identificados y priorizados, la adquisición de datos puede tener lugar.

Recolección de Datos

Se realizó un backup de la base de datos vía red, para ello se utilizó la Herramienta Acronis Reovery MS SQL Server y se utilizó este programa para la restauración de la misma en la estación forense.

- **Recolección de datos volátiles de la Base de Datos**

  Se utilizo la herramienta WFT, línea de comandos y la herramienta SQL Guifrontend, validación binaria y registro completo

Auditoria de la Base de Datos

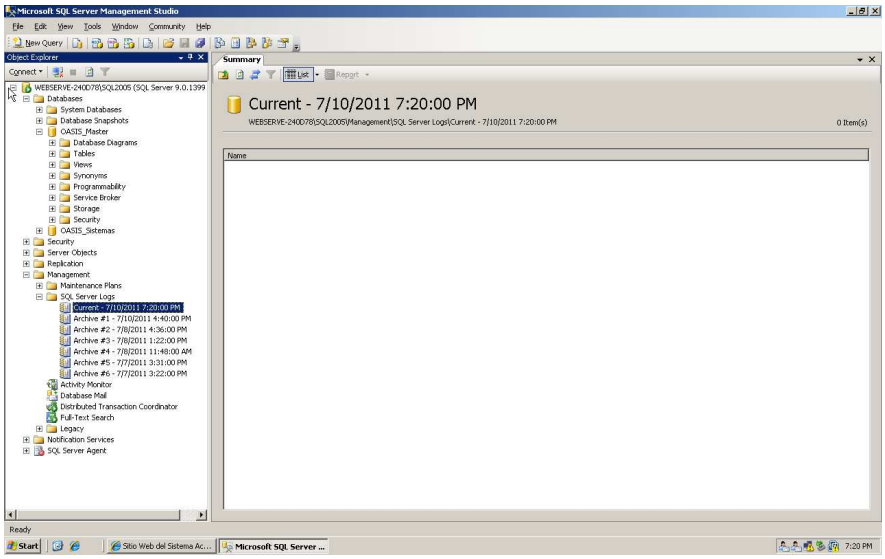


Figura VI.142. Registros de SQL

Falla al Ingresar al Servidor

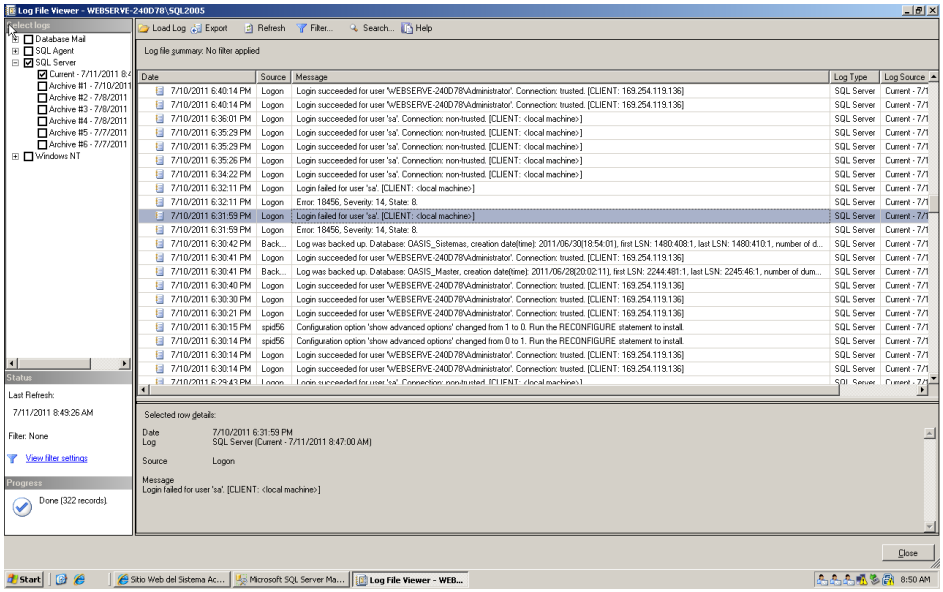


Figura VI.143. Falla ingreso al usuario sa

Ingreso Correcto al Servidor

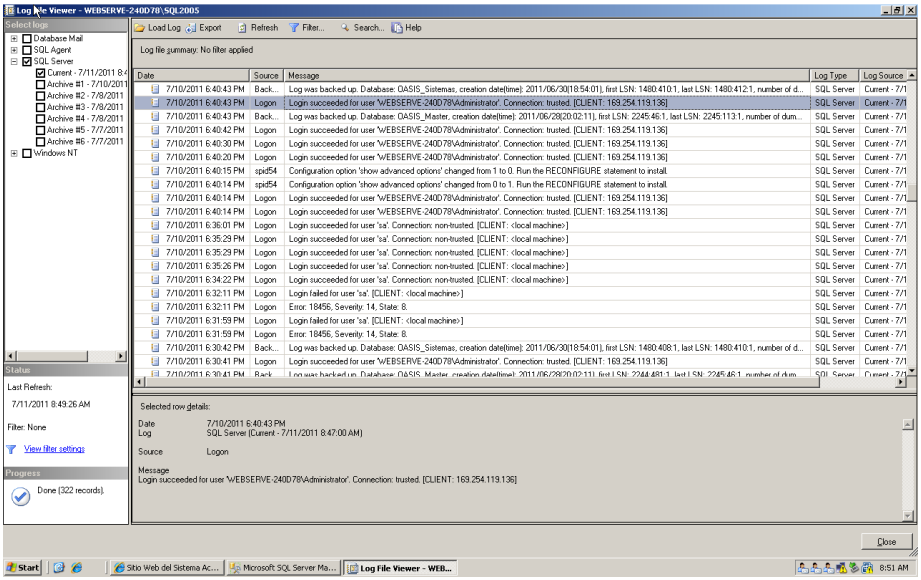


Figura VI.144. Ingreso satisfactorio al usuario sa.

Visor de Eventos

En el visor de eventos se visualizo todos los eventos realizados por las aplicaciones, nuestra información completa de todos los procesos que realizo el sistema indicando: fecha, hora, recurso, etc.

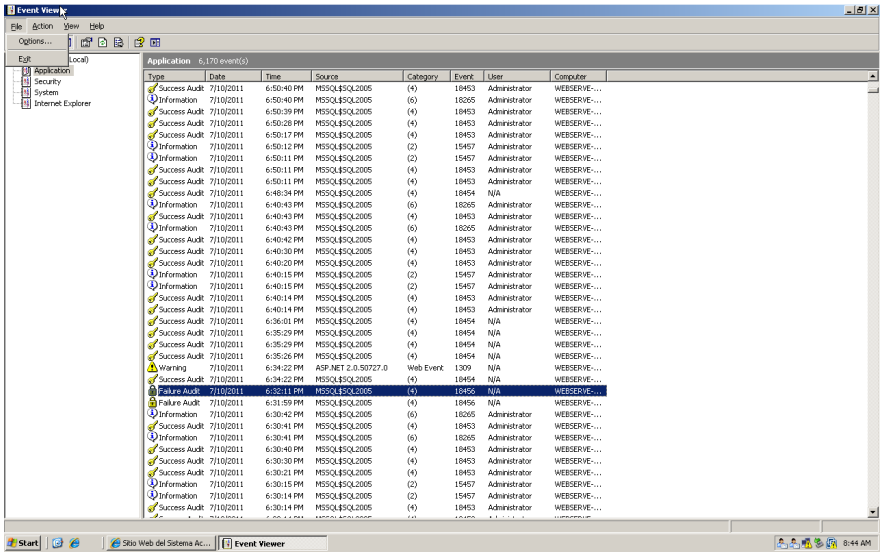


Figura VI.145. Ventana visor de eventos

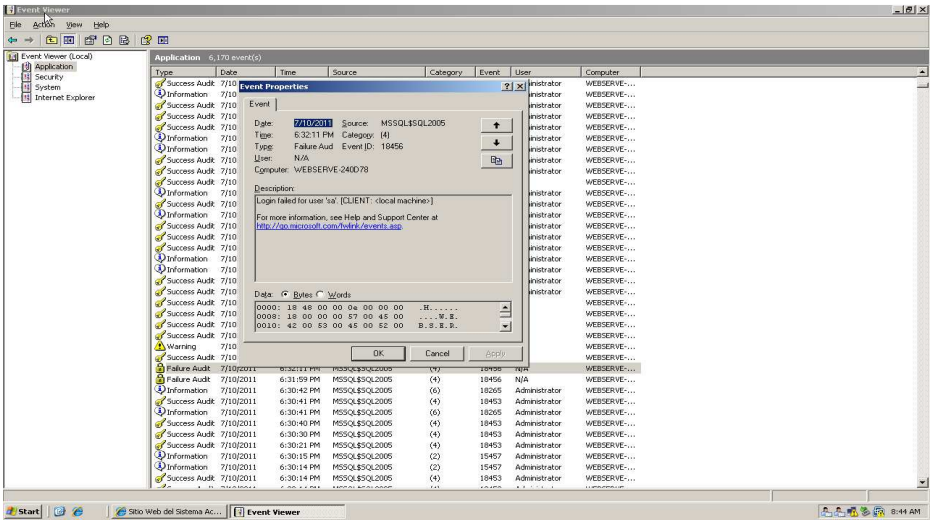


Figura VI.146. Propiedades de los eventos.

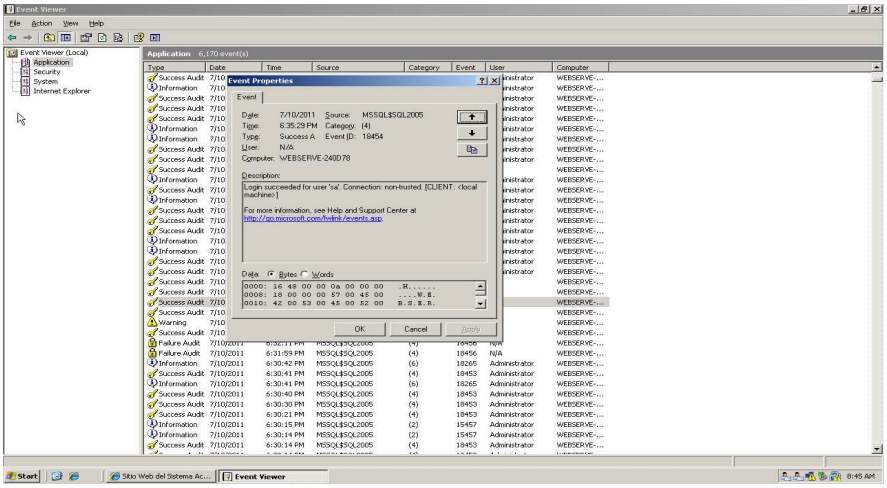


Figura VI.147. Evento login cerrado al usuario sa

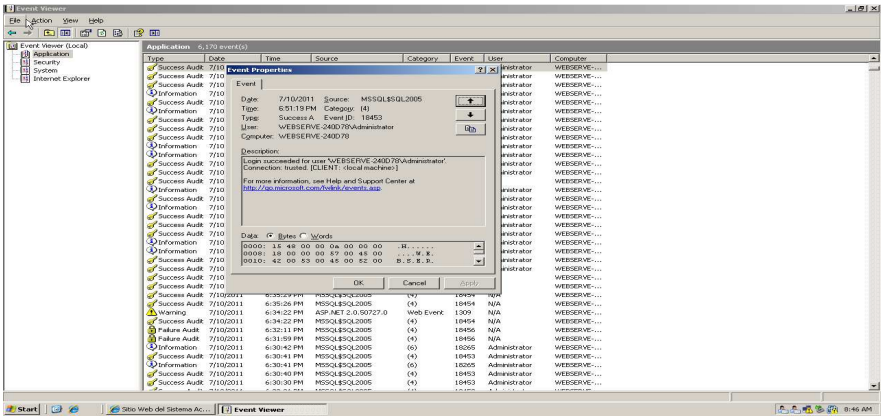


Figura VI.148 Evento login satisfactorio al usuario sa.

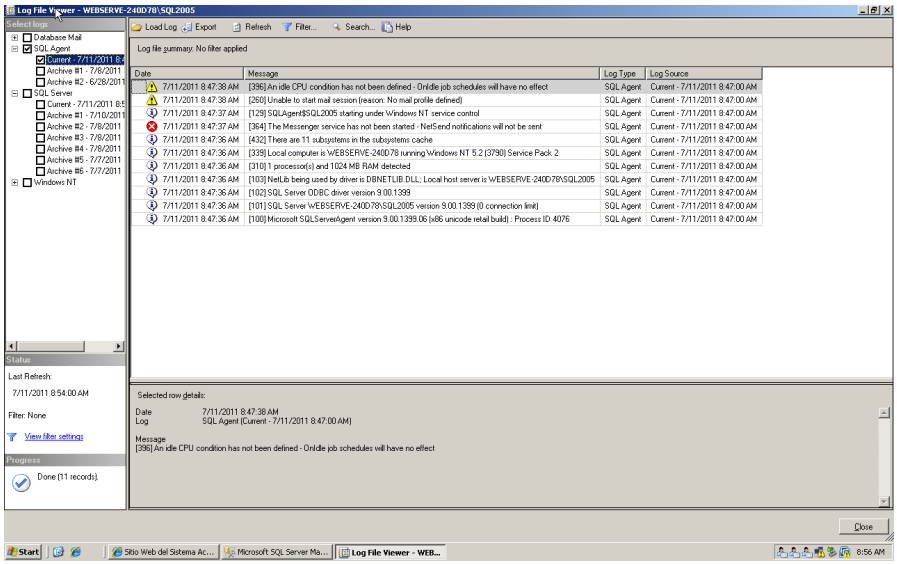


Figura VI.149. Visor de archivos log.

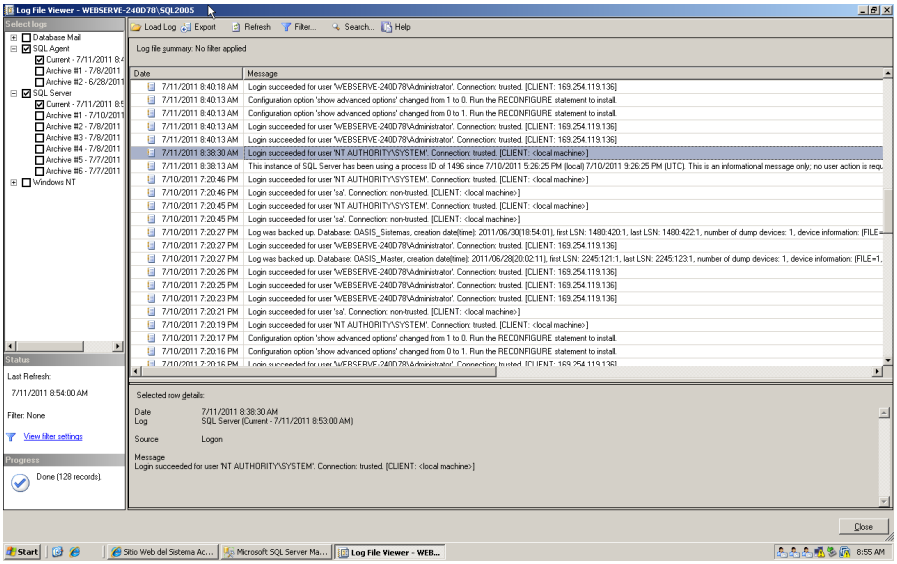


Figura VI.150. Inicio se sesión satisfactoria en el Visor de archivos Log

Priorización de Evidencia recogida

Se priorizo la evidencia de acuerdo a la tabla de Valores utilizados para determinar prioridad, una vez los datos han sido identificados y priorizados, la adquisición de datos puede tener lugar.

Recolección de Datos

Se realizo una copia imagen de los dispositivos (bit a bit), con una herramienta apropiada. En este caso se utilizo la herramienta Acronis Recovery for Ms SQL Server.

- **Recolección de datos volátiles de la Base de Datos**

  Se utilizo la herramienta WFT, línea de comandos y la herramienta SQL Guifrontend, validación binaria y registro completo

Recolectar Los Archivos De La Base De Datos Y Log

C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data

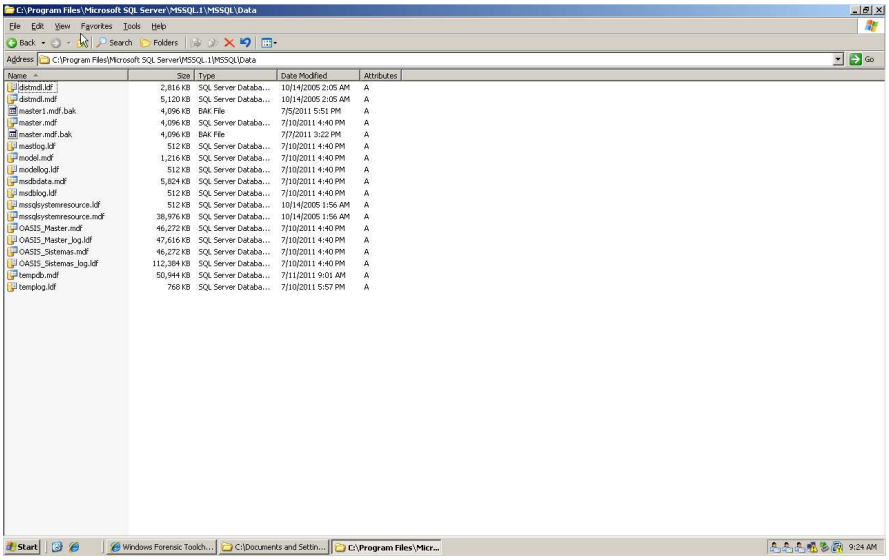


Figura VI.151. Archivos de la base de datos.

Recolectar los Archivos Trace por Defecto

C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG

C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG\log_55.trc

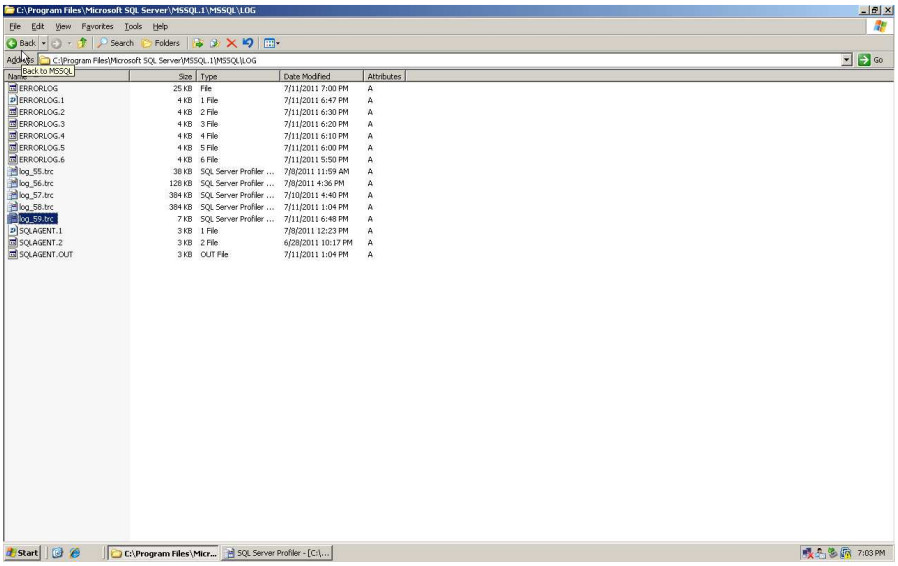


Figura VI.152. Archivos trace por defecto

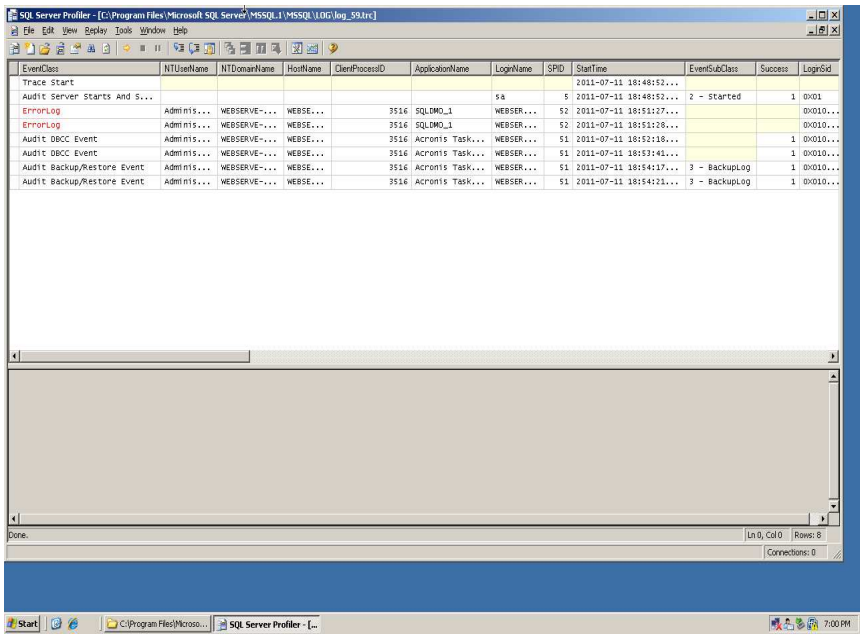


Figura VI.153. Archivos trace de la base de datos

Recolectar los Logs Error de SQL Server

C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG

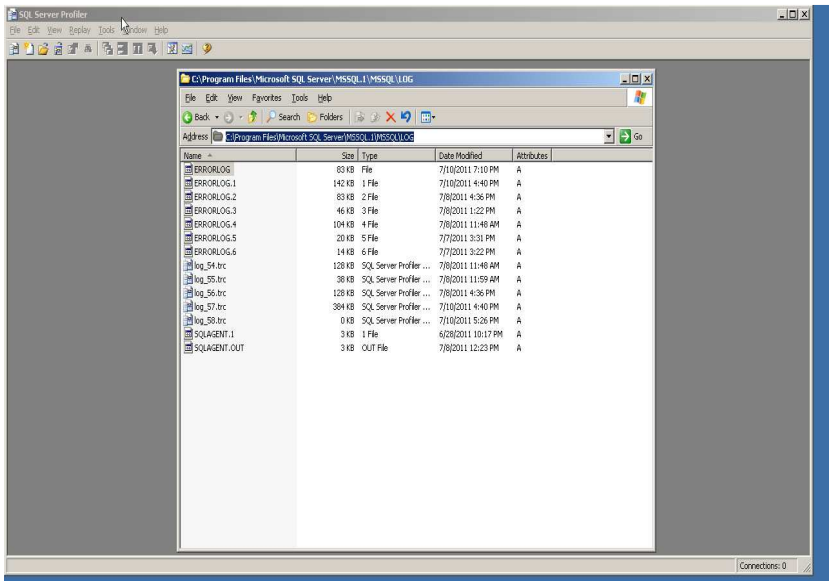


Figura VI.154 Logs error de SQL SERVER

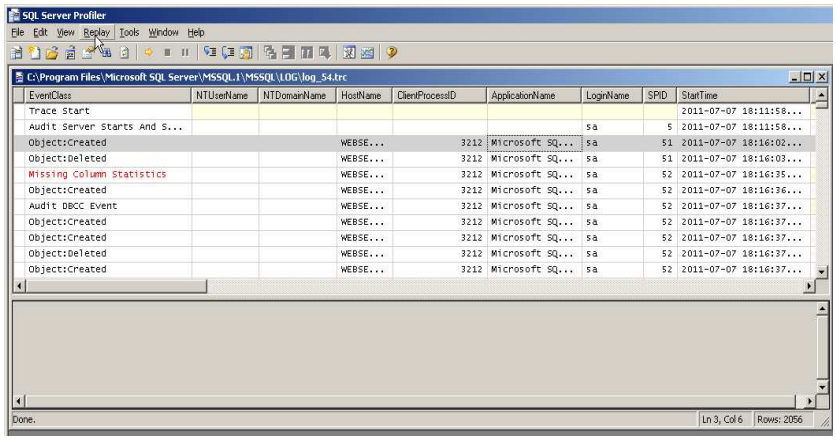


Figura VI.155. Archivo Logs error de SQL SERVER

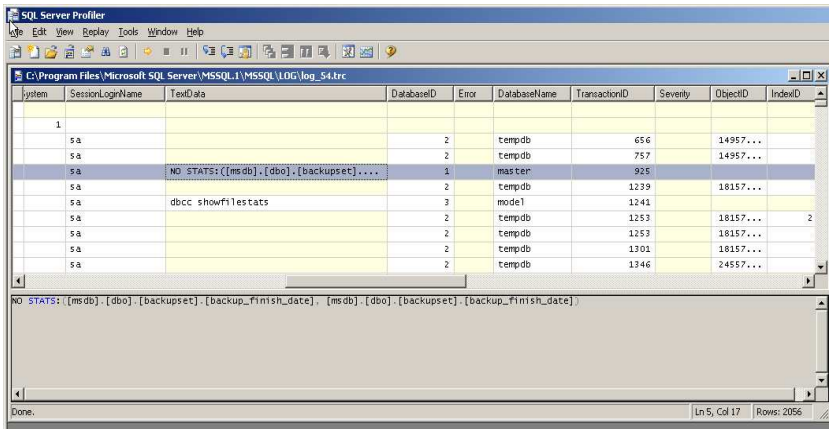


Figura VI.156. Detalles del archivo Logs error de SQL Server

Recolección de los Log Event del Sistema Com Wft

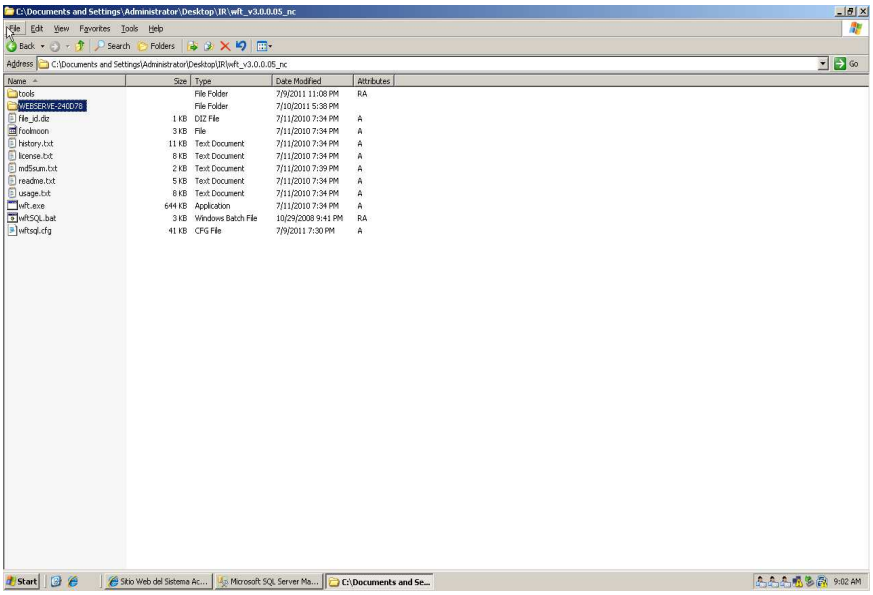


Figura VI.157. Carpeta WFT

Pantalla Principal de Windows Forensic Toolchest (WFT)

Figura VI.158. Pantalla Principal De Windows Forensic Toolchest

SQL Statement Data Cache

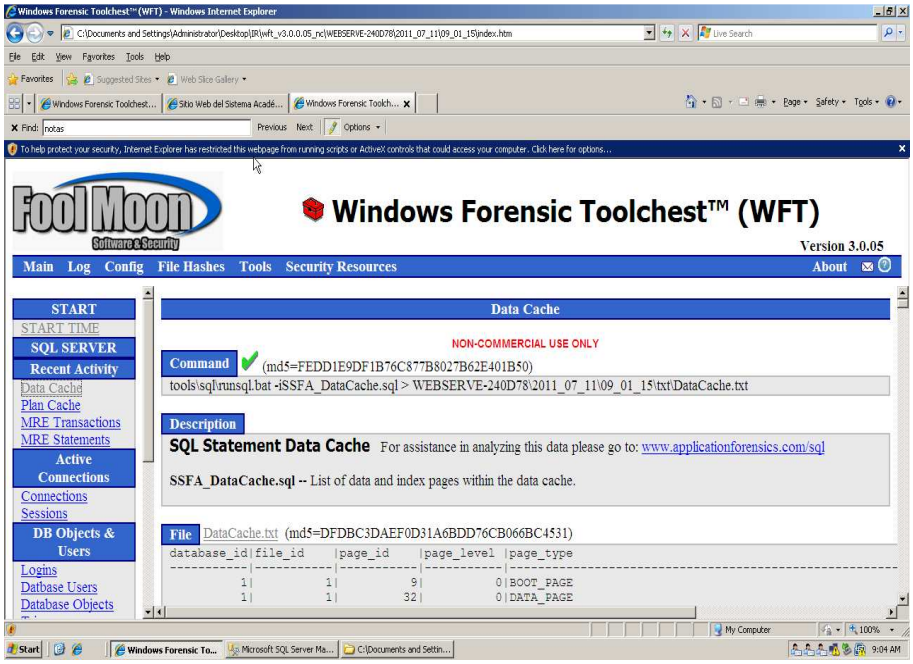


Figura VI.159. SQL Statement Data Cache

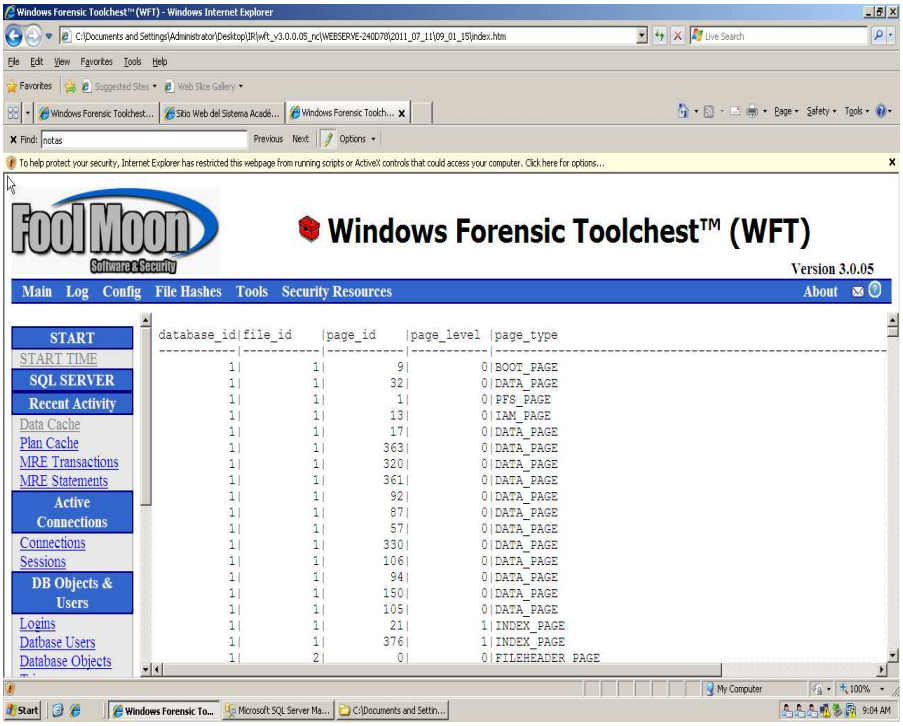


Figura VI.160. Ventana Data Cache

SQL SERVER Connections

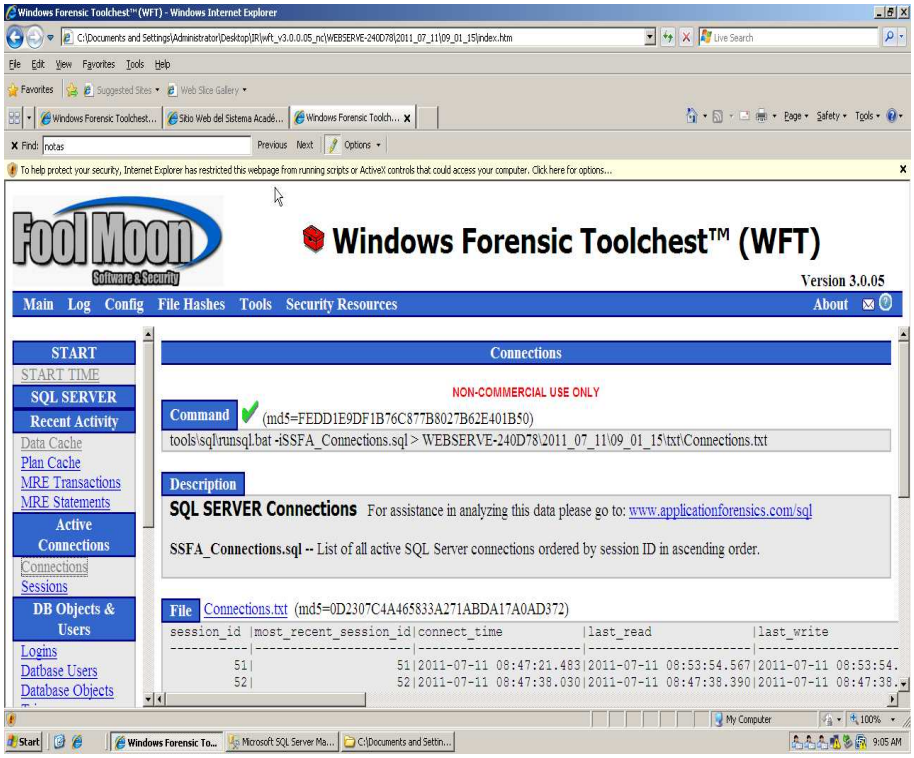


Figura VI.161. SQL Server Connections

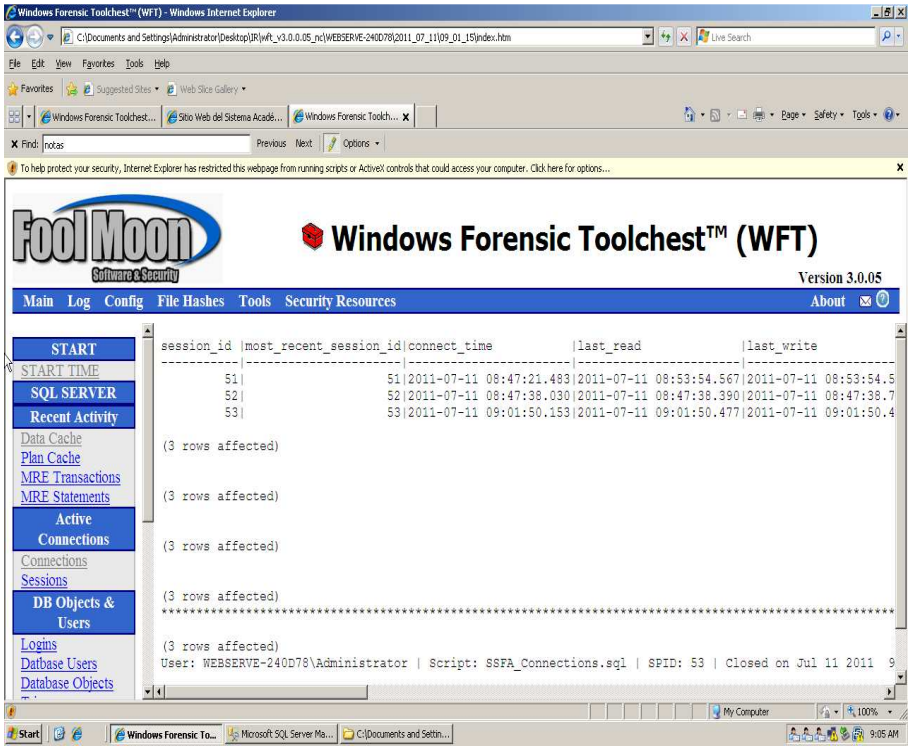


Figura VI.162 Ventana Connections

SQL SERVER Sessions

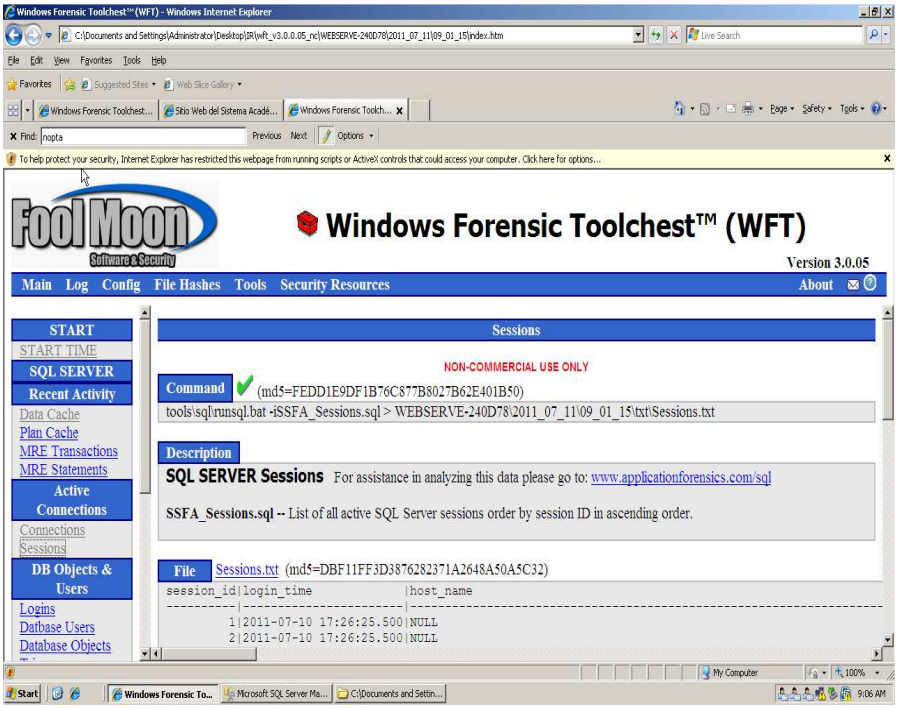


Figura VI.163. SQL Server Sessions

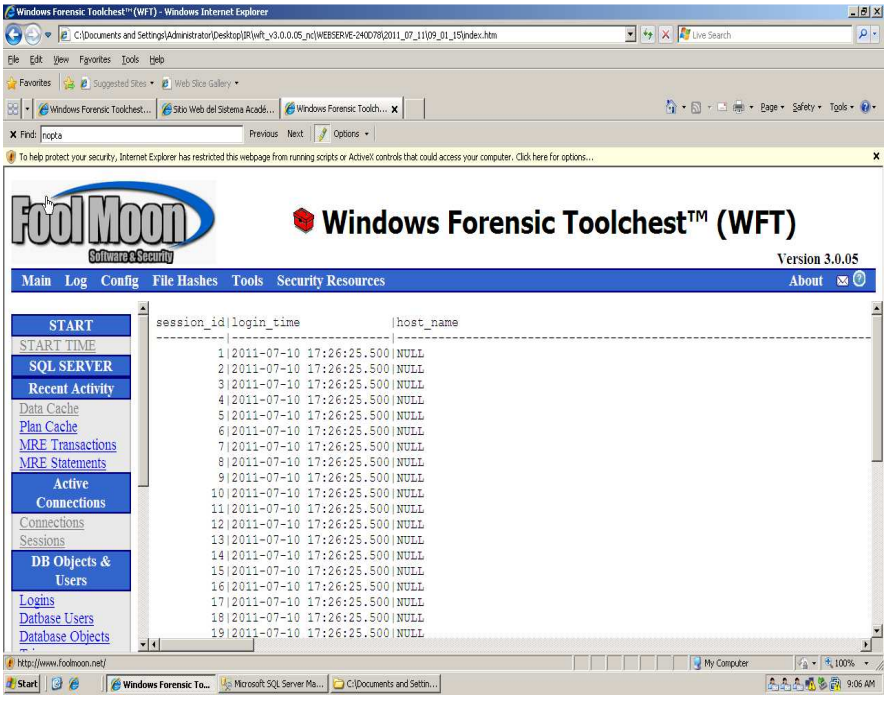


Figura VI.164. Ventana SQL Server Sessions

SQL SERVER Loggins

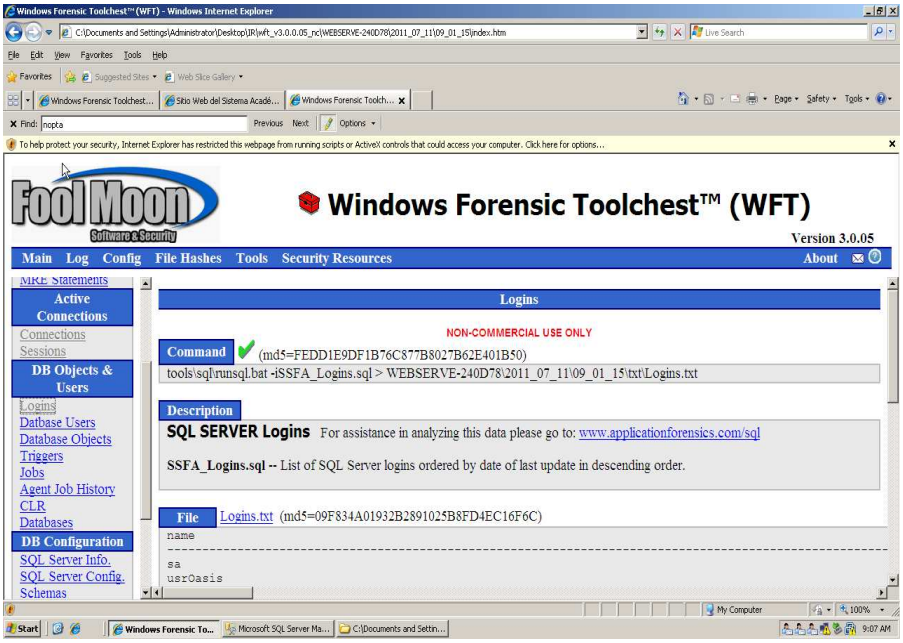


Figura VI.165. SQL Server Loggins

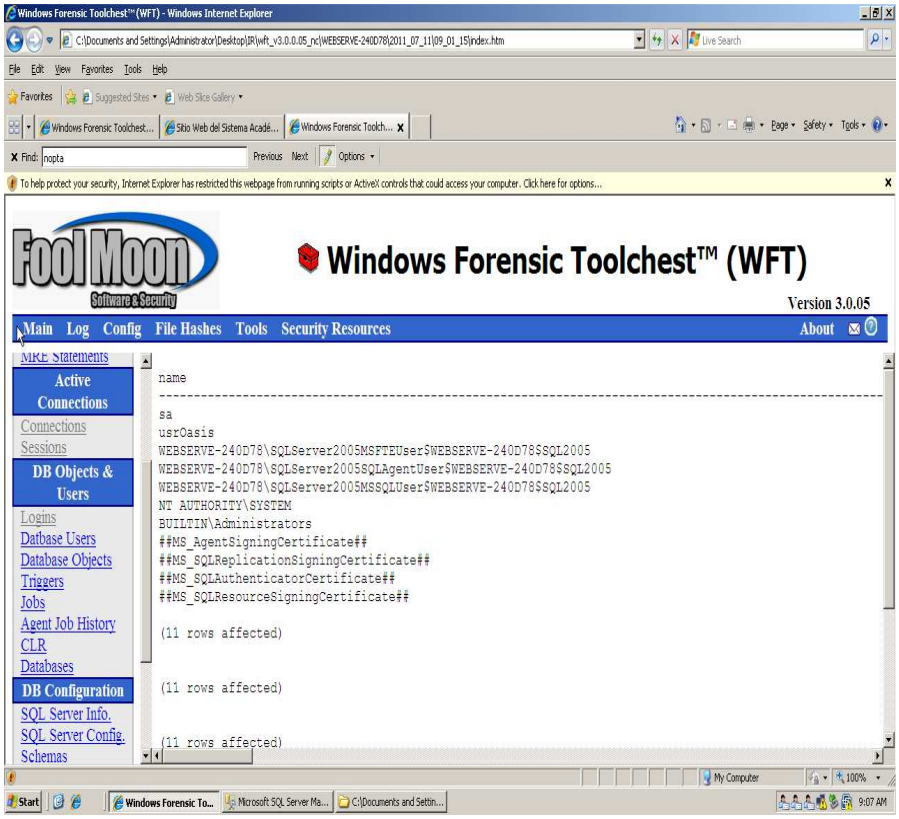


Figura VI.166. Ventana SQL Server Loggins

SQL SERVER Databases

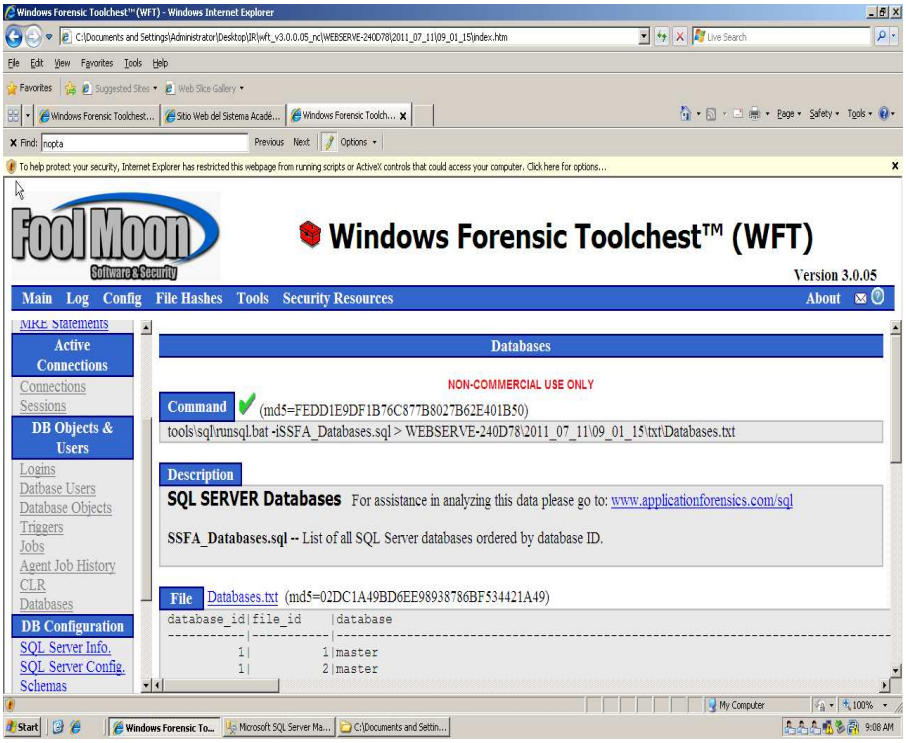


Figura VI.167. SQL Server Databases

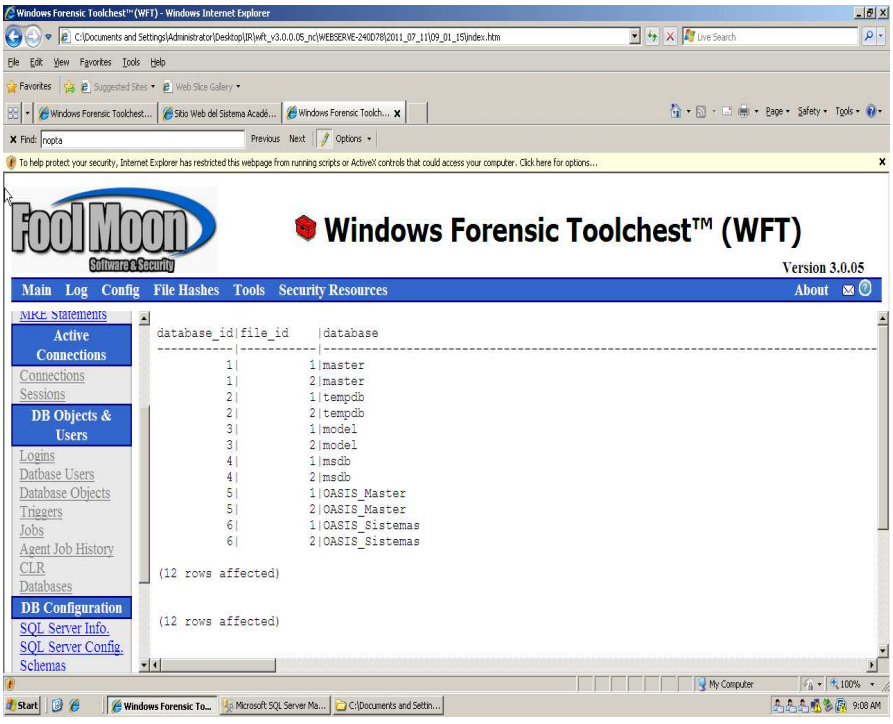


Figura VI.168. Ventana SQL Server Databases

Databases SERVER Informations

Figura VI.169. Databases Server Informations

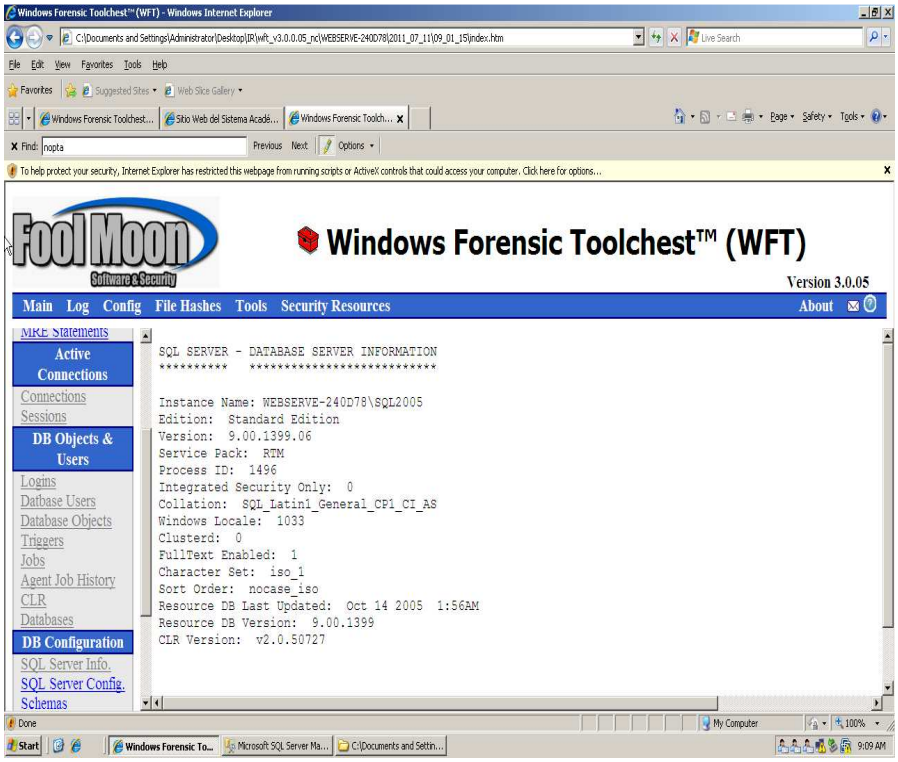


Figura VI.170. Ventana DBServerInfo

Eliminación de la tabla prueba de la base de datos oasis_master

PLAN CACHE Entries

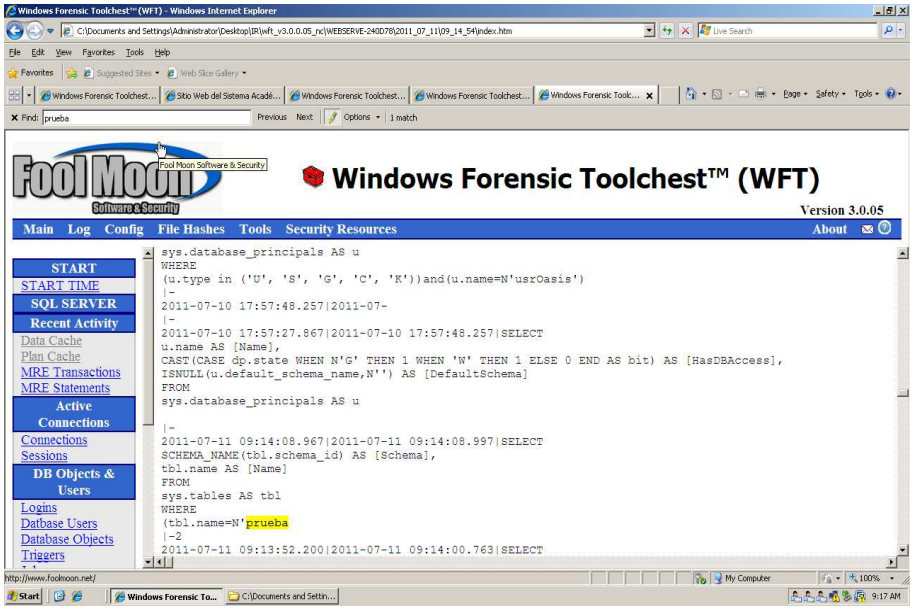


Figura VI.171. Plan Cache Entries

Eliminación de la Tabla nota con SQL Injection

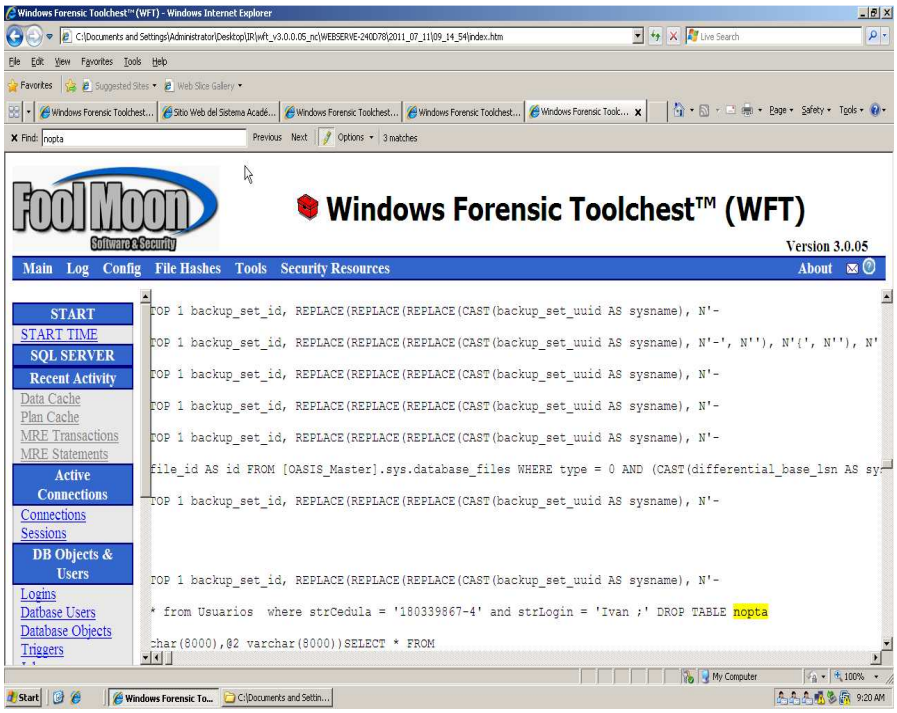


Figura VI.172. Eliminación de la tabla nota con SQL Injection

FASE IV: Análisis de Evidencia

1. **Analisis de Medios.** El cronograma establecido en la actividad anterior ahora se utilizo para establecer los limites en el análisis de medios.

   Se realizo un ánalisis de los registros de transacciónes de la base de datos, selecciónando las columnas que contienen los datos mas relevantes basados en el alcance de la investigación.

   - Registro de Eventos de Windows
     - Datos de Autenticación de SQL Server (fallas, inicio de seión y desconexion satisfactorios)
     - Apagado y Encendido de SQL Server
     - Direcciónamiento IP de conecciónes de cliente de SQL Server
   - Registro de Errores
     - Datos de Autenticación de SQL Server (fallas, inicio de seión y desconexion satisfactorios)
     - Apagado y Encendido de SQL Server
     - Direcciónamiento IP de conecciónes de cliente de SQL Server
   - Seguimiento Predeterminado de la Base de Datos
     - Historial de autenticación completa
     - Operaciónes DLL (Esquema de cambios)
     - Direcciónamiento IP de conecciónes de cliente de SQL Server
   - Archivoc Log y Archivos de Datos
     - Archivos adjuntos
     - Usar para obtener información de un esquema on-demand, contenido de pagina de datos,etc.
   - Registro de Transacciónes Activas
     - Importación a Excel/ Acceso para revision
     - Identificar sentecias DML y DDL
     - Mapa de transacciónes para un SPID
   - Registro de Transacción – Operaciónes de Actualización
   - La página DBCC recogerá la página modificada
   - Revisión de la cabecera de la página detectará el objeto
   - Recolectar el objeto esquema

A través del análisis, se identifico toda la información relacionada con aquellos objetos considerados sobresalientes. De igual forma, se identifico cuáles son las características que presenten esos objetos. Al final de esta fase y por consecuencia, se debió contar con una lista de características para cada pieza de información que resulte de interés.

Se aplicaron las Herramientas de Detección de Vulnerabilidades y se realiza las respectivas interpretaciones

Fase V. Recuperación de Datos

- En cuanto a la recuperación de datos se utilizo la herramienta Acronis Recovery for MS SQL server
- Para el análisis forense se utilizó las siguientes herramientas
- WINDOWS FORENSIC TOOLSCHEST en la cual viene incluida md5 y sqlcmd
- La seguridad de SQL SERVER 2005 en cuanto a auditoria de inicio de sesión

RESTAURACIÓN DE LA BASE DE DATOS

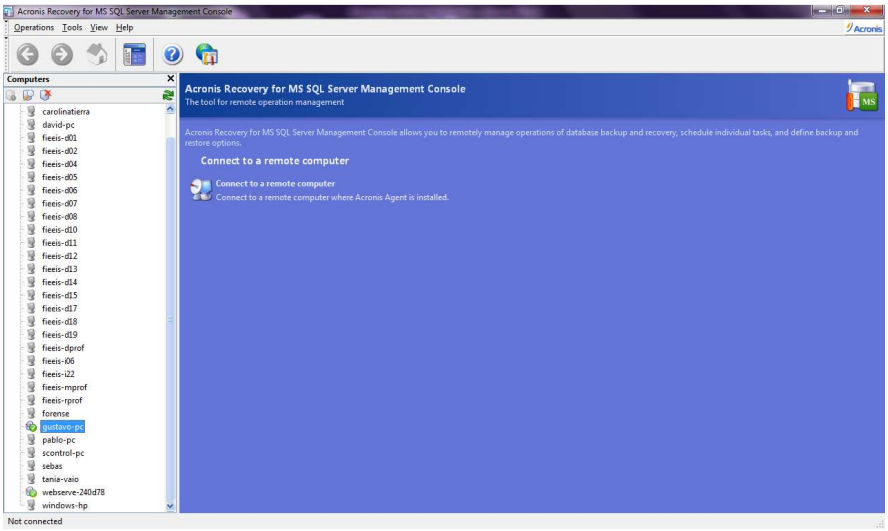


Figura VI.173. Ventana principal de Acronis Recovery For MS SQL

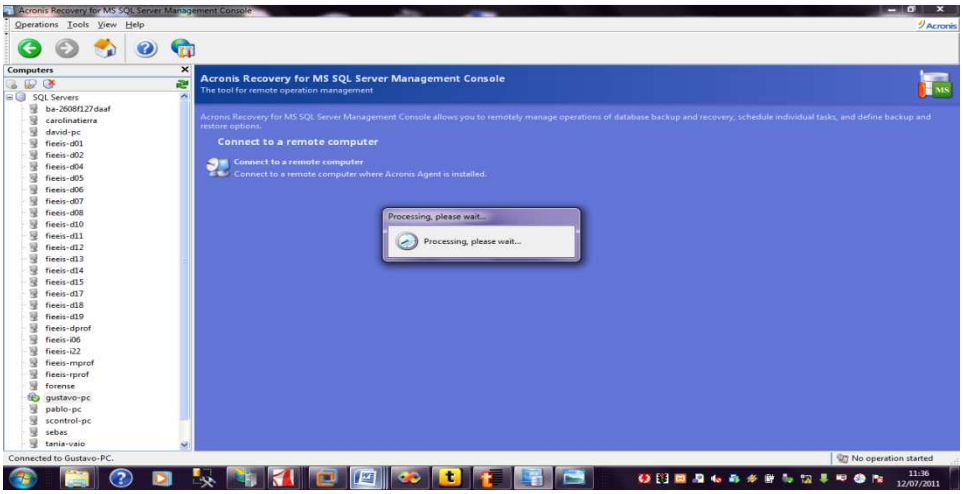


Figura VI.174. Conexión remota

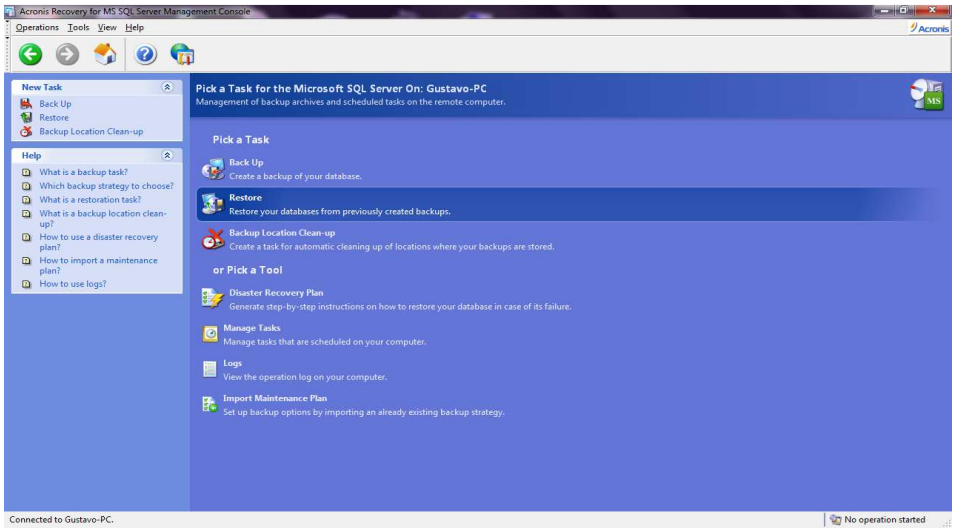


Figura VI.175. Lista de tareas

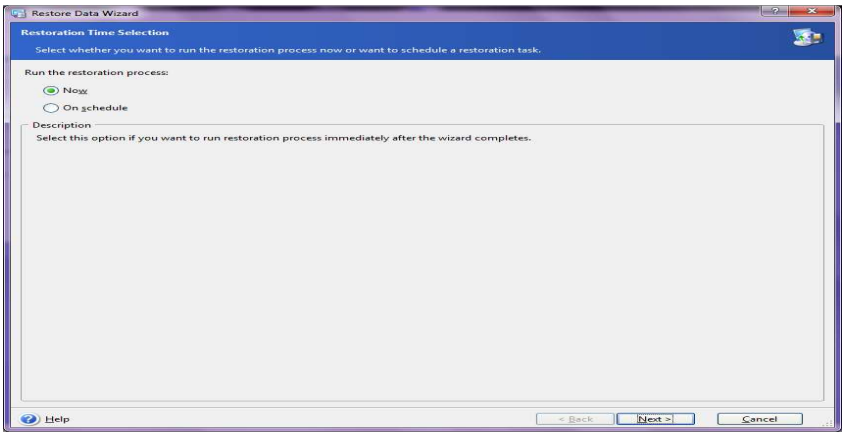


Figura VI.176. Tiempo de restauración.

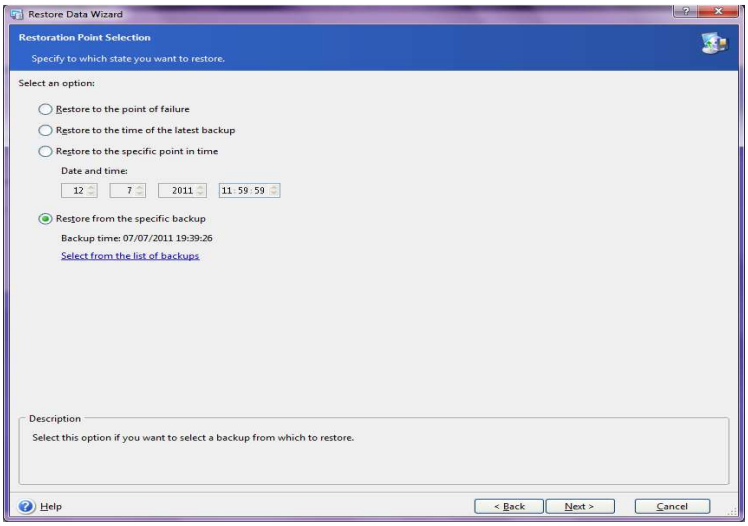


Figura VI.177. Punto de restauración.

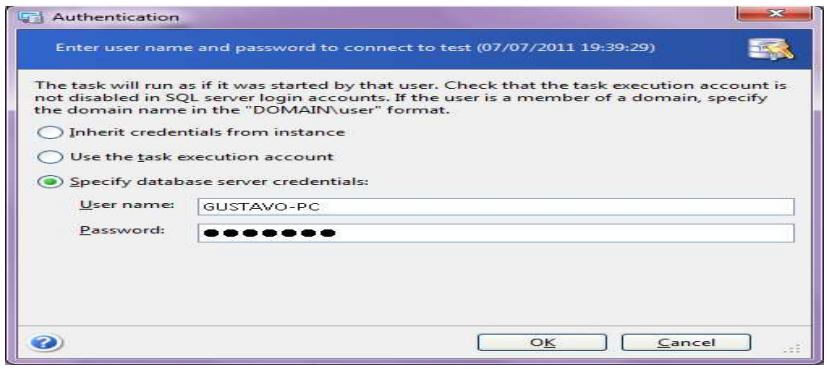


Figura VI.178. Autenticación

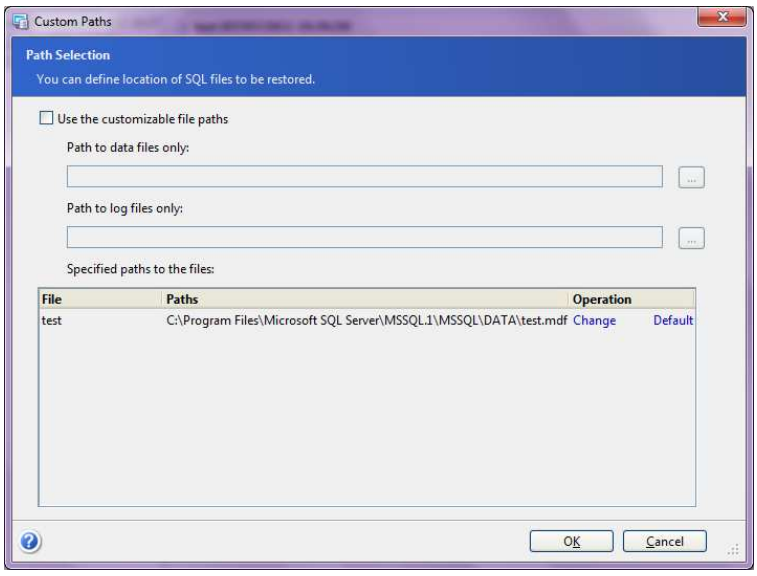


Figura VI.179. Ruta del archivo

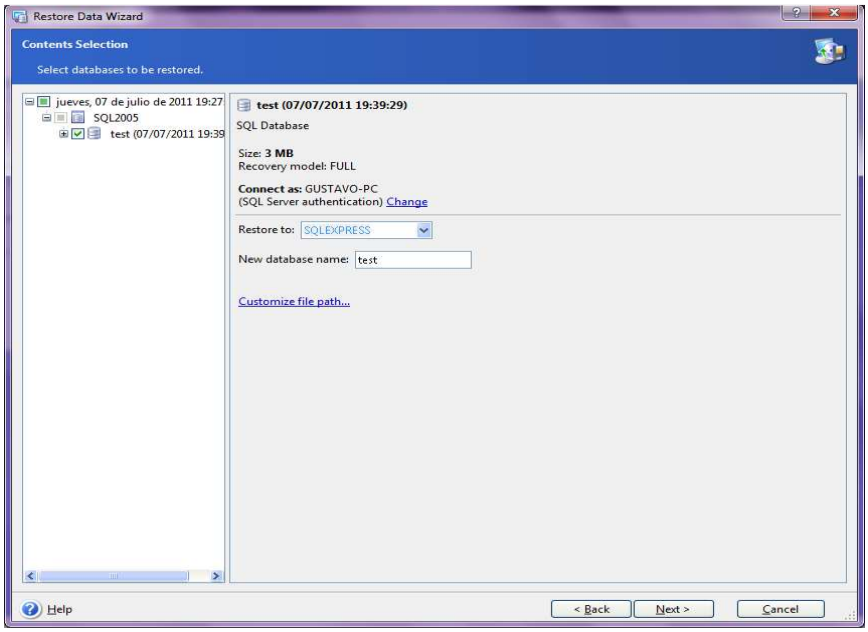


Figura VI.180. Base de datos a restaurar

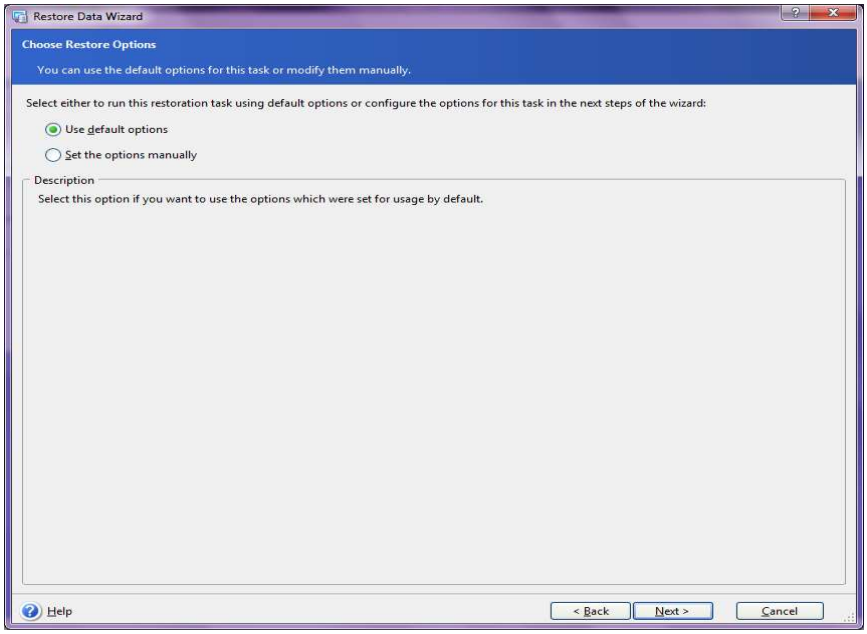


Figura VI.181. Opciones de restauración

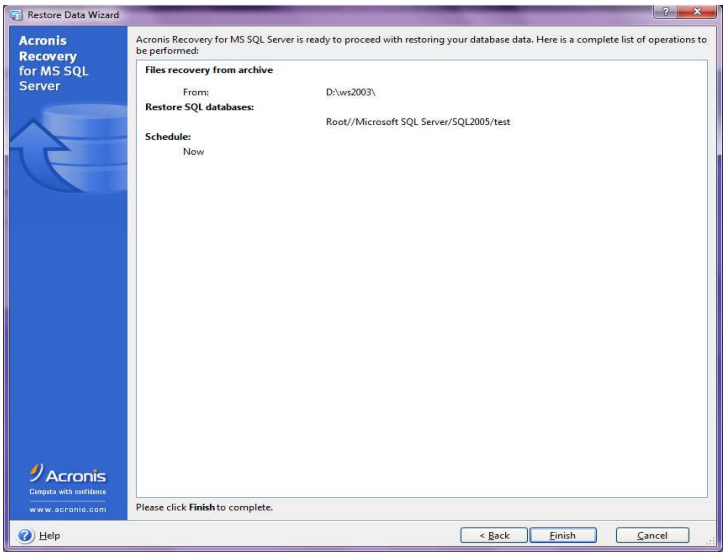


Figura VI.182. Restauración completada.

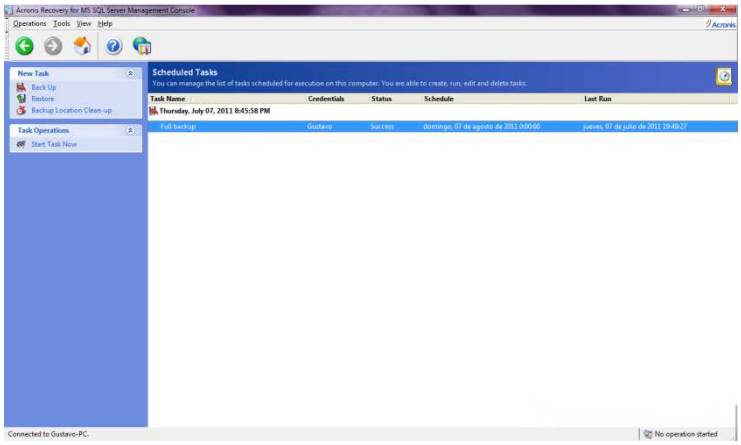


Figura VI.183. Ventana de tareas

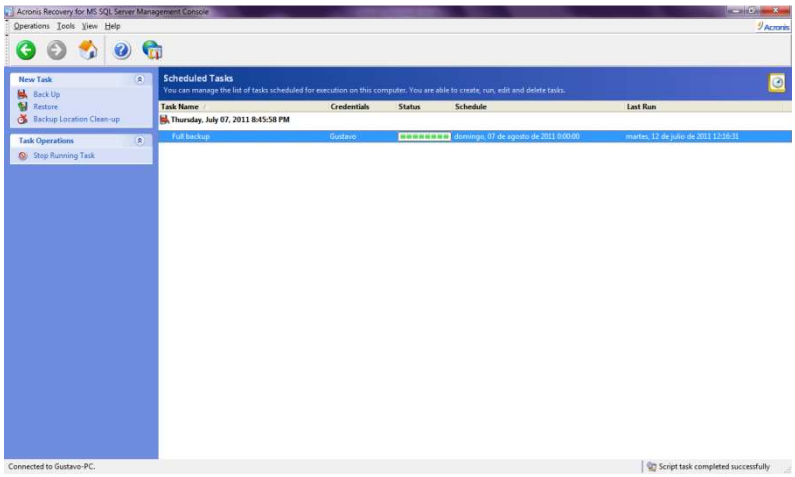


Figura VI.184. Tarea completada

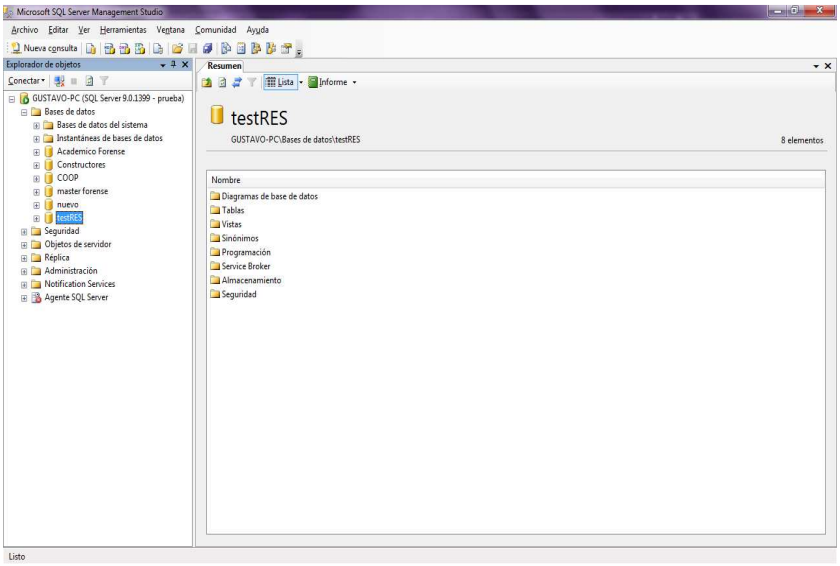


Figura VI.185. Ingreso a la base de datos restaurada

6.8. CONCLUSIÓN DEL INFORME PERICIAL

- La evidencia digital se ha preservado en el proceso de tal manera que no ha sido alterada ya que se ha trabajado con la copia de la base de datos, dejando intacta la base de datos original.
- La base de datos restaurada muestra que hubieron acciones erróneas de ingreso de sesión
- Mediante el análisis del reporte generado por WINDOWS FORENSIC TOOLSCHEST se puede observar toda la información del servidor de base de datos
- Conjuntamente con el registro de entrada y videos tomadas en DESITEL y los resultados del informe como son las cuentas de usuario, la hora, y la fecha en la cual se ejecuto la acción maliciosa se muestra lo siguiente:

  System Name: WEBSERVE-240D78

  Operating System: Microsoft Windows Server 2003 family, Advanced Server 5.2 Service Pack 2 (Build 3790)

  User Name: Administrator

  Windows Directory: C:\WINDOWS

  System Directory: C:\WINDOWS\system32

  System Date/Time: 07/11/2011 09:14:54 (24h)

  *2011-07-10 18:36:47.150|2011-07-10 18:36:47.163|select * from Usuarios where strCedula = '180339867-4' and strLogin = 'Ivan ;' DROP TABLE nopta;SELECT * FROM usuarios WHERE strLogin LIKE '%'*

*|0x060005008169112CB8E150050000000000000000000000 |5 |1 |020000008169112C8AD73D04AA3DEEC373156883C5BF1A92 2011-07-10 18:24:19.663|2011-07-10 18:36:47.150|(@1 varchar(8000),@2 varchar(8000))SELECT * FROM [Usuarios] WHERE [strCedula]=@1 AND [strLogin]=@2 |0x06000500169C7427B821DA0900000000000000000000000000 |5 |1 |02000000169C74274A6F6E642F432797A7C5EE6E6B28D4DC 2011-07-10 18:34:22.693|*

*2011-07-10 18:34:22.693|select * from Usuarios where strCedula = '180339867-4' and strLogin = 'Ivan ;' DROP TABLE nota;SELECT*

Cuenta de usuario: *sa*

Fecha de eliminación: *2011-07-10 18:34:22.693*

Acción realizada: *DROP TABLE nota;SELECT*

6.9. POSIBLES SOLUCIONES PARA EVITAR ATAQUES A LA BASE DE DATOS

1. Para evitarlo debemos implementar una serie de funciones php que filtren las entradas de los usuarios, una posible función sería la siguiente:

```
<?
Function secureSQL( strVar )
    dim banned, final, i

    banned = array("select", "drop", ";", "--", "insert","delete", "xp_")

    for i = 0 to uBound(banned)
        strVar = replace(strVar, banned(i), "")
    next

    final = replace(strVar, "'", "''")
    secureSQL = final
End Function
?>
```

Mediante esta función filtramos todos los caracteres extraños de la sentencia, evitando así un caso como el anteriormente comentado.
Una función que también nos será de gran utilidad para evitar éste tipo de ataques es la función **addslashes.**

2. Usar una cuenta con permisos restringidos a la base de datos

Otro dato importante a tener muy en cuenta es asegurarnos de que la cuenta de usuario utilizada por nuestra aplicación tiene los permisos necesarios para poder acceder y/o modificar unos datos concretos pero también que sea lo suficiente restrictiva para no alterar otro tipo de datos.

3. No mostrar al usuario la información de error generada por la base de datos

En muchos casos los mensajes de error pueden ser lo suficientemente descriptivos como para que el usuario se percate de información acerca de la estructura de la base de datos.

4. Rechazar las peticiones con caracteres sospechosos

Tabla IV.XXXI Caracteres Sospechosos

Carácter especial	**Significado SQL**
;	Delimitador de consultas.
‘	Carácter delimitador de cadena de datos.
-	Comentario.
/* */	Delimitadores de comentario. El texto entre /* y */ no es evaluado.
xp_	Se utiliza en el inicio del nombre de procedimientos almacenados extendidos de catálogo, como xp_cmdshell.

5. Al crear el usuario de DB restringir el mismo a las funciones básicas y necesarias para el correcto funcionamiento de nuestra aplicación.
Habilitar a nuestro usuario a ejecutar cláusulas como “DROP” es una potencial vulnerabilidad y raramente son necesarias en nuestras aplicaciónes.

Efectuar consultas concretas (Ej: “SELECT `nombre`,`apellido` FROM…”) y evitar el abuso del “SELECT * FROM…”.

Raramente necesitamos traer todos los datos de una tabla, tupla o columna, traer los justos y necesarios va a reforzar la seguridad en nuestra aplicación y a optimizar el tiempo de ejecución de la misma. En este caso obtenemos un doble beneficio.
No desplegar errores en pantalla a los usuarios de la aplicación.
La salida de errores en pantalla puede develar información clave de la estructura de nuestra DB poniendo en compromiso la seguridad de nuestra aplicación. Podemos utilizar la función “error_reporting” para ocultar errores y posteriormente utilizar el manejo de exepciónes de PHP para definir errores personalizados y guardarlos en un log privado.

6. Validar los datos que ingresan via formulario con PHP.

Las validaciones con JAVASCRIPT pueden ser fácilmente burladas y en algunos casos basta con deshabilitar el javascript del navegador.

7. Filtrar TODOS los datos que recibimos.

Validar que sean enteros o cadenas, asegurarnos de filtrar caracteres impropios como operadores aritméticos (Ej: *,-,+,=,%,etc) , escapar las comillas con contrabarras (Ej: utilizando funciones como “mysql_real_escape_string” o “addslashes“) y convertir los textos en entidades html utilizado “htmlentities“.

8. Reservar palabras.

Filtrar y prohibir palabras equivalentes a clausulas SQL como “INSERT, DROP, DELETE, SELECT, UPDATE, UNION, etc”.
En este caso tendremos que ser muy selectivos, ya que muchas palabras son de normal uso (Ej:”UNION”) y si estamos programando una aplicación en inglés ni que hablar.
Nunca responda a solicitudes de información personal a través de correo electrónico.
Mantenga su sistema operativo actualizado.
Maneje un gestor de correo electrónico con funciones anti-spam que borre directamente del servidor el correo no deseado.

Tras recibir un mail con un fichero adjunto no lo ejecute hasta analizarlo con un antivirus.

Sepa que es mucho más seguro tipear la URL de un banco que acceder al mismo a través de un enlace.

Tenga precaución con aquellas entidades con las que intercambie información sensible y no dispongan de certificación de autentificación.

Avise a su banco o entidad cada vez que haya sido vícitima de un ataque Phishing.

Use el sentido común, es la mejor herramienta de protección frente a cualquier tipo de ataque de seguridad.

En cuanto a la prevención se puede tener en cuenta lo siguiente:

9. Mantener en buen estado de seguridad el equipo utilizado para la administración del sitio Web:

Disponer de software actualizado, así como herramientas de seguridad instalada y actualizada (antivirus, antiespías, etc.)

10. Auditar constantemente el sitio Web habilitando la opción de "logs permanentes":

De esta forma, el log de acceso al sitio guarda las conexiones recibidas vía HTTP o FTP.

11. Buena política de contraseñas seguras:

Elegir contraseñas fuertes y seguras para dificultar la toma de control de los sitios, correos electrónicos, FTPs, etc.

12. Disponer de copias de seguridad de la Web:

En muchos casos, puede ahorra tiempo reemplazar el código dañado por copias del mismo que se sepan limpias. Sin embargo, haciendo esto se destruyen las evidencias de cómo ocurrió el ataque y cómo evitar que vuelva a ocurrir, salvo si realizamos una copiad e seguridad de la Web o sitio comprometido tras el ataque.

13. Compartir información con servidores de terceros:

Esta es una práctica que suele darse en portales transaccionales que tienen externalizados ciertos servicios como el registro en base de datos u otras operaciones.

En estos casos, se debe controlar cómo se transfieren los datos entre los servidores (encriptados, etc.) para que no sean interceptados. Además, todas las validaciones deben hacerse en el servidor para que no sean modificables desde la parte cliente (navegador).

14. Comprobar que los permisos de ficheros y directorios son seguros:

- Chequear que los permisos de los archivos del sitio Web son los correctos.
- No dar permisos totales a carpetas que no los necesiten para no facilitar la creación de ficheros maliciosos.
- Gestionar correctamente los permisos asignados a cada usuario.

Actualizar el software tanto del servidor web como de la plataforma es muy importante para evitar ataques.

15. Buena programación de la Web, usando código seguro:

Consiste en utilizar buenas técnicas de programación Web para evitar vulnerabilidades susceptibles de ser explotadas. Requiere estar familiarizado con el código fuente y las peculiaridades de las plataformas utilizadas.

Los exploits utilizados más comúnmente en los ataques son:

- LFI, Local File Inclusion
- RFI, Remote File Inclusion
- Inyecciónes SQL

16. Mantener el software empleado (servidor Web, bases de datos, etc.) en las últimas versiones:

Elaborar una lista de todos los programas de terceros que se usan y asegurarse de que se encuentren actualizados a la última versión o versión sin vulnerabilidades conocidas.

Los fabricantes suelen disponer de enlaces en sus páginas oficiales que permiten la actualización de su software.

17. Bloquear la actividad sospechosa a través de los archivos de configuración distribuida:

Añadir determinadas líneas en los archivos de configuración, según se pretenda restringir el acceso a directorios, ISP, IPs, etc., manejar errores del servidor, controlar la caché, etc. Una buena configuración puede evitar intentos de ataque RFI.

Un ejemplo puede ser el archivo *".htaccess"* (*public_html/.htaccess*):

```
AuthName "Directorio Protegido"
AuthUserFile /ruta/.htpasswd
AuthType basic
Require valid-user "Directorio Protegido"
```

6.10. ANÁLISIS DE RESULTADOS Y COMPROBACIÓN DE LA HIPÓTESIS

La hipótesis planteada pertenece a una hipótesis de Investigación específicamente de Causa- Efecto ya que esta diferencia dos tipos de variables:

V. DEPENDIENTES.- Dependen del valor de la variable independiente

V. INDEPENDIENTES.-Son manipuladas por el investigador.

Para nuestro estudio se ha considerado la siguiente hipótesis y variables

HIPÓTESIS

La aplicación de la guía de técnicas y procedimientos de análisis forense permitirá obtener evidencias consistentes y facilitará la detección de vulnerabilidades.

Tabla IV.XXXII Hipótesis

VARIABLE INDEPENDIENTE		**VARIABLES DEPENDIENTES**	
X	La aplicación de la guía de técnicas y procedimientos de análisis forense	**Y**	Consistencia de evidencias
		Z	Facilidad de detección de vulnerabilidades

PROCESO DE COMPROBACIÓN DE LA HIPÓTESIS

Comprobación Variable Y: Consistencia de evidencias

Para la comprobar la consistencia de las evidencias se procede a utilizar los valores de hash MD5 de los datos recogidos antes y después del análisis son los mismos. Por lo tanto, la evidencia recogida es creíble, confiable, repetible y aceptable para los interesados en la Investigación forense. Además se puede verificar si hay la misma cantidad de elementos (tablas, vistas, registros, procedimientos, etc.) de la base de datos analizada y su backup realizado vía red y que se encuentra en la estación forense son iguales.

Tabla IV.XXXIII Consistencia de Evidencia

		ANTES	DESPUES	TOTAL (%)
Consistencia de evidencias	Número de tablas	87	87	100%
	Número de procedimientos almacenados	154	154	100%
	Número de vistas	24	24	100%
	Número de funciones	43	43	100%
	Número de tipos de datos definidos por el usuario	39	39	100%
	Número de reglas	11	11	100%
	Número de valores predeterminados	36	36	100%
	Tamaño del archivo MDF	45,1 MB	45,1 MB	100%

Tabla IV.XXXIV Consistencia de Evidencia en función de valores Hash

Evidencia Adquirida	Tipo de Archivo	Valor Hash MD5(Antes de Analizar)	Valor Hash MD5(Después de Analizar)	Integridad Mantenida (Si, No)
DataCache.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
PlanCache.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
Tlog.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
RecentStatements.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
Connections.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
Sessions.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
Logins.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
DbUsers.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
DatabaseObjects.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
Triggers.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
Jobs.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
JobHistory.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
CLR.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
Databases.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
DBServerInfo.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
Configuration.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
Schemas.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
Endpoints.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
AutoExecProcs.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
Time.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si
ClockHands.txt	Texto	D41D8CD98F00B204E9800998ECF8427E	D41D8CD98F00B204E9800998ECF8427E	Si

La obtención de evidencias consistentes utilizando la guía de procedimientos propuesta es un 100% por ende la evidencia recogida es creíble, confiable y aceptable.

Comprobación Variable Z: Facilidad de detección de vulnerabilidades
Para la comprobación de esta variable se toma en cuenta el número de herramientas de detección que facilita conocer las vulnerabilidades expuestas en la siguiente tabla.

Valoración

ALTO $\rightarrow$ 3
MEDIO $\rightarrow$ 2
BAJO $\rightarrow$ 1

La valoración se hará en base al nivel de detección de vulnerabilidades que ofrecen las herramientas analizadas en el capítulo 4, de acuerdo a la Tabla IV.XXI y la Tabla IV.XXII, se revisa los promedios obtenidos por cada vulnerabilidad y se un valor de acuerdo a un rango establecido en el Anexo 14.

Tabla IV.XXXV Facilidad de detección de vulnerabilidades

		Nivel
Facilidad de detección de vulnerabilidades	SQL Inyección	3
	Detección de puertos abiertos	3
	Contraseñas débiles	2
	Acceso a elementos de la BD (tablas, procedimientos, vistas, etc.)	3
	Otros (Framework, Memoria, etc.)	3

$$x = \frac{14 \times 100}{15} = 93{,}33\%$$

Se obtuvo una suma de 11 puntos que equivale al 93.33% de facilidad de detección de vulnerabilidades utilizando la guía de procedimientos propuesta.

RESULTADOS

- Con la utilización la guía de procedimientos se obtendrá una consistencia de la evidencias en un 100%, mientras que se facilitará en un 93.33% la detección de vulnerabilidades en un Servidor de Base de datos en el cual se aplique el análisis forense.

- Una vez analizado los datos obtenidos, se tiene como conclusión final que la aplicación de la guía de técnicas y procedimientos de análisis forense permitirá obtener evidencias consistentes y facilitará la detección de vulnerabilidades en un Servidor de Base de Datos, dando como cierta la hipótesis planteada.

CONCLUSIONES

- La mejor herramienta para la recuperación y restauración de base de datos es Acronis Recovery for MS SQL SERVER en relación a la funcionalidad con un porcentaje del 98%, la misma que fue utilizada para la obtención de la copia de la base de datos del Sistema Académico y restauración .
- El Análisis Forense en bases de datos actualmente depende de las herramientas propias de cada sistema manejador de base de datos(DBMS), puesto que no existen en el mercado herramientas dirigidas a recolectar evidencias en una Base de Datos.
- Uno de los aspectos mas importantes es la captura y la interpretación de evidencias siendo Windows Forensic Toolchest una herramienta excelente de análisis forense porque ayuda a buscar señales de un incidente, de intrusos, o para confirmar el mal uso del equipo.
- Si la evidencia es recogida de manera adecuada habrá mayores posibilidades de establecer una ruta hacia los atacantes y contar con mayores elementos probatorios en el evento de una persecución y juzgamiento del intruso.
- Actualmente existen muy pocas herramientas para detección de vulnerabilidades en Base de Datos, y las existentes tienen costos muy elevados, la cual es una de las razones porque las empresas o instituciones no poseen la seguridad adecuada en sus Servidores de Base de Datos.
- La guía de procedimientos de Análisis Forense fue aplicada en un escenario diseñado exclusivamente para simular ataques y vulnerabilidades reales dentro del contexto de una Base de Datos SQL Server 2005. En este punto, el enfoque fue dirigido a explorar la eficiencia de la guía propuesta, así como su efectividad frente a la evidencia encontrada y los reportes presentados, viabilidad y limitantes de aplicación.
- Con la aplicación de la guía de procedimientos se obtendrá una consistencia de la evidencias en un 100%, y se facilitará en un 90% la detección de vulnerabilidades en un Servidor de Base de datos en el cual se aplique el análisis forense, por lo tanto la hipótesis planteada para esta investigación se acepta luego de una análisis de datos y verificación de parámetros.

- La guía propuesta de esta investigación se construyo en base a 4 modelos de análisis forense como son: modelo DFRW, modelo abstracto, modelo CFFTPM y el modelo básico de los cuales se tomo las fases las relevantes especialmente del modelo básico.

RECOMENDACIONES

- Se debe mantener la evidencia intacta por lo cual se debe realizar una copia o backup de la base de datos dañada.

- Al finalizar un análisis forense informático es necesario elaborar un informe para proporcionar toda la información relevante de las evidencias de forma clara, concisa, estructurada y sin ambigüedad para hacer la tarea de asimilación de la información fácil y establecer la conclusión de la pericia.

- Aplicar técnicas forenses para obtener, analizar, recopilar cualquier evidencia del ataque, esto es muy valioso para utilizar herramientas automáticas que nos asistan en el proceso de análisis forense.

- Al momento de elegir una herramienta para recuperar los elementos de una base de datos o detectar vulnerabilidades, se recomienda realizar una selección de acuerdo a los resultados obtenidos mediante el análisis comparativo realizado en la investigación.

- Se recomienda realizar otros temas de tesis derivados de este tema, ya que el campo de analisis forense es muy amplio y necesario para descubrir incidentes de seguridad en el campo informatico, actualmente existen estudios relacionados con oracle y framework.

RESUMEN

El estudio de esta tesis es elaborar, aplicar y evaluar una guía metodológica de Análisis forenses en la Base de Datos del Departamento de Sistemas y Telemática (DESITEL) de la ESPOCH. Esta investigación se realiza con el fin de facilitar al personal técnico la recolección y análisis de evidencia digital que se produce durante un incidente de seguridad en un Servidor de Base de Datos SQL Server y MySQL.

Se utilizó herramientas hardware como equipo computacional y herramientas software para recuperación de información. Se aplicó el método científico y analítico y como fuentes de información páginas web, observación y experimentación.

La guía de procedimientos se estructuro en 6 fases con un orden preestablecido: Identificación en la cual se deberá descubrir la ocurrencia del incidente, Verificación se asegura la escena para evitar accesos no autorizados, Recolección de Evidencia se procede a recolectar la evidencia sin alterarla, Análisis de Evidencia en la que se crea un backup de la base de datos con la herramienta Acronis Recovery For Ms SQL Server, en la cual se establecieron cuatro escenarios obteniendo un 100% de funcionalidad de esta manera se consiguió no alterar la información, Recuperación de datos se recupera la información de la base de datos afectada y la fase de Preparación de informe en la que se describe todo el proceso y los resultados obtenidos. Con la utilización la guía de procedimientos se facilitará en un 91.67% la detección de vulnerabilidades en un Servidor de Base de datos.

Se concluyó que, la aplicación de la guía de procedimientos de análisis forense optimiza la recolección de evidencias.

Se recomienda utilizar correctamente la guía de procedimientos para obtener, analizar y recopilar cualquier evidencia del ataque de forma que sean legalmente aceptadas en cualquier proceso legal.

SUMMARY

To elaborate, apply, and evaluate a methodological guide of forensic analysis of the System and Telematics Database Department (DESITEL) at the ESPOCH is the proposal of this thesis study. This research is carried out to make easy to the technicians the collecting and digital analysis evidence produced during a security incidence in a Server of Database SQL Server and MySQL.

Hardware tools were used such as computer and software to recover information. The scientific and analytic method was applied and web pages, observation and experimentation as information source.

The guide of procedures was structured in phases with a pre-established order: Identification to discover the evidence, Verification to assure the stage to avoid unauthorized access, Recollecting of Evidence without changing, Evidence Analysis to create a backup of database with the tool Acronis Recovery for Ms Sql Server, where four stages were established getting 100% of function, therefore the information did not change, Recovering of data, getting the information of database affected and the phase of Preparation of a report where the process and the obtained result are described. The detecting of vulnerabilities in a Database Server will be feasible in a 91.67% with the use of the process guide.

It was concluded that with the application of the forensic analysis procedure guide the collecting of evidences are getting better.

It is recommended to use the procedure guide to obtain, analyze and collect any attack evidence legally accepted in any legal process.

GLOSARIO

Active Directory: El Directorio Activo (Active Directory) es la pieza clave del sistema operativo Windows Server, sin él muchas de las funcionalidades finales de este sistema operativo(las directivas de grupo, las jerarquías de dominio, la instalación centralizada de aplicaciones, etc.), no funcionarían.

ActiveX Data Objects (ADO): Conjunto de objetos COM para el acceso a recursos de datos. Prevee una capa entre los lenguajes de programación y las bases de datos OLE, lo que permite a los programadores escribir programas que accedan a datos, sin saber cómo está implementada la base de datos (sólo se debe tener cuidado en la conexión a la misma).

Almacén de datos: es una colección de datos orientada a un determinado ámbito (empresa, organización, etc.), integrado, no volátil y variable en el tiempo, que ayuda a la toma de decisiones en la entidad en la que se utiliza. Se trata, sobre todo, de un expediente completo de una organización, más allá de la información transaccional y operacional, almacenado en una base de datos diseñada para favorecer el análisis y la divulgación eficiente de datos (especialmente OLAP, procesamiento analítico en línea).

Archivos temporales: Aplicaciones de escritorio de Windows, como Write y varias aplicaciones de MDI (interfaz) de documento, como Excel, crean archivos temporales para controlar la edición de usuarios necesarios.

ASP: Active Server Pages, también conocido como ASP clásico, es una tecnología de Microsoft del tipo "lado del servidor" para páginas web generadas dinámicamente, que ha sido comercializada como un anexo a Internet Information Services (IIS).

Backdoors (Puerta trasera): Defecto en un software o página web que permite ingresar a un recurso que usualmente está restringida a un usuario ajeno. No siempre es un defecto (bug), también puede ser una entrada secreta de los programadores o webmasters con diversos fines.

Backup (Copia de seguridad): Es la copia total o parcial de información importante del disco duro, CDs, bases de datos u otro medio de almacenamiento. Esta copia de respaldo debe ser guardada en algún otro sistema de almacenamiento masivo, como ser discos duros, CDs, DVDs o cintas magnéticas (DDS, Travan, AIT, SLR,DLT y VXA).

Búffer: Espacio de memoria que se utiliza como regulador y sistema de almacenamiento intermedio entre dispositivos de un sistema informático. Así, por ejemplo, las impresoras suelen contar con un buffer donde se almacena temporalmente la información a imprimir, liberando a la memoria del ordenador de dichos datos, y permitiendo que el usuario pueda seguir trabajando mientras se imprimen los datos. También existen buffers entre diferentes dispositivos internos del ordenador.

Cache del Sistema: Un caché es un sistema especial de almacenamiento de alta velocidad. Puede ser tanto un área reservada de la memoria principal como un dispositivo de almacenamiento de alta velocidad independiente. Hay dos tipos de caché frecuentemente usados en las computadoras personales: memoria caché y caché de disco.

Cadena de custodia: Define como el procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de administrar justicia y que tiene como fin no viciar el manejo de que ellos se haga y así evitar alteraciones, sustituciones, contaminaciones o destrucciones.

Cifrado: Es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

Claves asimétricas: es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella.

C**ookie:** es un fragmento de información que se almacena en el disco duro del visitante de una página web a través de su modo a petición del servidor de la página. Esta información puede ser luego recuperada por el servidor en posteriores visitas.

Credenciales: Es un registro que contiene la información de autenticación (credenciales) necesaria para conectarse a un recurso situado fuera de SQL Server. Esta información es utilizada internamente por SQL Server. La mayoría de las credenciales incluyen un nombre de usuario y una contraseña de Windows.

DBA: es la persona responsable de los aspectos ambientales de una base de datos

DLL (DynamicLinking Library): Es la implementación de Microsoft del concepto de bibliotecas (librerías) compartidas en sistemas Windows y OS/2. Generalmente estas bibliotecas llevan la extensión ".dll" o ".ocx" (para aquellas que contienen controles ActiveX), o ".drv" (controladores de sistema).

Encriptación: Es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

Filtros de Contenido: permite a las empresas asegurar un uso consecuente de la red de banda ancha que tienen instalada en su oficina. De esta manera, se reduce el tiempo de uso personal que utilizan los empleados en las aplicaciones de comunicaciones de Internet, el acceso a contenidos web o la descarga de ficheros.

Hash: En informática, hash se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. Un hash es el resultado de dicha función o algoritmo.

IDS: (intrusión detection system o IDS) Sistema que detecta manipulaciones no deseadas en el sistema, especialmente a través de internet. Las manipulaciones pueden ser ataques de hackers malintencionados.

Intranet: Es una red de ordenadores privados que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales. El término intranet se utiliza en oposición a Internet, una red entre organizaciones, haciendo referencia por contra a una red comprendida en el ámbito de una organización

Kernel: En informática, un núcleo o kernel (de la raíz germánica Kern) es un software que constituye la parte más importante del sistema operativo. Es el principal responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma más básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema

Log: Archivo que registra movimientos y actividades de un determinado programa (log file). En un servidor web, se encarga de guardar todos los requerimientos (“requests”) y servicios entregados desde él, por lo que es la base del software de estadísticas de visitas.

MD5: es uno de los algoritmos de reducción criptográficos diseñados por el profesor Ronald Rivest del MIT (Massachusetts Institute of Technology, Instituto Tecnológico de Massachusetts). Fue desarrollado en 1991 como reemplazo del algoritmo MD4 después de que Hans Dobbertin descubriese su debilidad.

MDAC: Microsoft Data Access Components (MDAC) es un framework de tecnologías interrelacionadas desarrollado por Microsoft que permite a los programadores una manera uniforme y exhaustiva de desarrollar aplicaciones que puedan acceder casi cualquier almacén de datos.

Medio Electrónico: Mecanismo, instalación, equipamiento o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones, incluyendo cualquier red de comunicación abierta o restringida como Internet, telefonía fija y móvil o de otros

Mensajería Instantánea: Es una forma de comunicación en tiempo real entre dos o más personas basada en texto. El texto es enviado a través de dispositivos conectados a una red como Internet.

Metadata: Es definido comúnmente como "los datos acerca de los datos", en el sentido de que se trata de datos que describen cual es la estructura de los datos y como se relacionan.

OLAP: Procesamiento Analítico En Línea es una solución utilizada en el campo de la llamada Inteligencia empresarial (o Business Intelligence) cuyo objetivo es agilizar la consulta de grandes cantidades de datos.

OLTP: Es un tipo de proceso especialmente rápido en el que las solicitudes de los usuarios son resueltas de inmediato; naturalmente, ello implica la concurrencia de un «mecanismo» que permite el procesamiento de varias transacciones a la vez.

ODBC: Orígenes de Datos es un estándar de acceso a bases de datos, que permite mantener independencia entre los lenguajes de programación, los sistemas de bases de datos y los sistemas operativos.

Roles: Papel que desempeña una persona o grupo en cualquier actividad.

Servidores de Logs: (server log), uno o más ficheros de texto automáticamente creados y administrados por un servidor, en donde se almacena toda la actividad que se hace sobre éste. Cada servidor, dependiendo de su implementación y/o configuración, podrá o no crear determinados logs.

SHA1:(Secure Hash Algorithm, Algoritmo de Hash Seguro) es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el NationalInstitute of Standards and Technology (NIST). El primer miembro de la familia fue publicado en 1993 es oficialmente llamado SHA. Sin embargo, hoy día, no oficialmente se le llama SHA-0 para evitar confusiones con sus sucesores.

Socket: Es un método para la comunicación entre un programa del cliente y un programa del servidor en una red. Un socket se define como el punto final en una conexión. Los sockets se crean y se utilizan con un sistema de peticiones o de llamadas de función a veces llamados interfaz de programación de aplicación de sockets (API, application programming interface)

Tablas de enrutamiento: Es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad. Dado que se trata de encontrar la mejor ruta posible, lo primero será definir qué se entiende por mejor ruta y en consecuencia cuál es la métrica que se debe utilizar para medirla

Transact-SQL: Es una extensión del lenguaje SQL, propiedad de Microsoft y Sybase. La implementación de Microsoft funciona en los productos Microsoft SQL Server. En tanto, Sybase utiliza el lenguaje en su Adaptative Server Enterprise, el sucesor de Sybase SQL Server.

Uptime: Muestra la hora actual, el número de días que el PC está encendido, número de usuarios conectados al equipo, carga media del equipo.

URL: Un localizador uniforme de recursos, más comúnmente denominado **URL** (sigla en inglés de uniform resource locator), es una secuencia de caracteres, de acuerdo a un formato modélico y estándar, que se usa para nombrar recursos en Internet para su localización o identificación, como por ejemplo documentos textuales, imágenes, vídeos, presentaciones, presentaciones digitales, etc.

Validación: Es la acción y efecto de validar **(**convertir algo en válido**,** darle fuerza o firmeza). El adjetivo válido, por otra parte, hace referencia a aquello que vale legalmente o que es firme y subsistente.

ANEXOS

ANEXO 1

ROLES GENÉRICOS PROPUESTOS POR LA NIST

El NIST (Instituto Nacional de Estándares y Tecnologías) propone una serie de roles genéricos los cuales se nombran a continuación:

- **Personal de emergencia:** Es personal entrenado, el cual llega de 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.

- **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.

- **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 acciónes 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.

- **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.

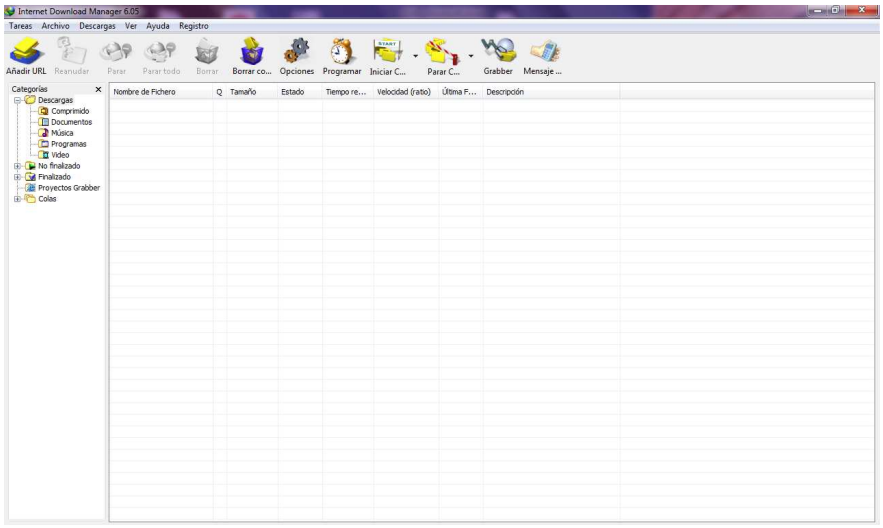
- **Examinadores forenses:** Son personal especialmente entrenado para reproducir las imágenes digitales adquiridas y recuperar los datos que se puedan obtener. Los examinadores son los encargados de hacer visible la potencial evidencia digital en el dispositivo. Ellos también pueden adquirir datos más difíciles de obtener utilizando herramientas altamente especializadas, realizando ingeniería reversa u otros métodos que no están disponibles para los técnicos forenses. Generalmente no es recomendable tener personas que tengan los roles de técnicos y examinadores al mismo tiempo.

- **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.

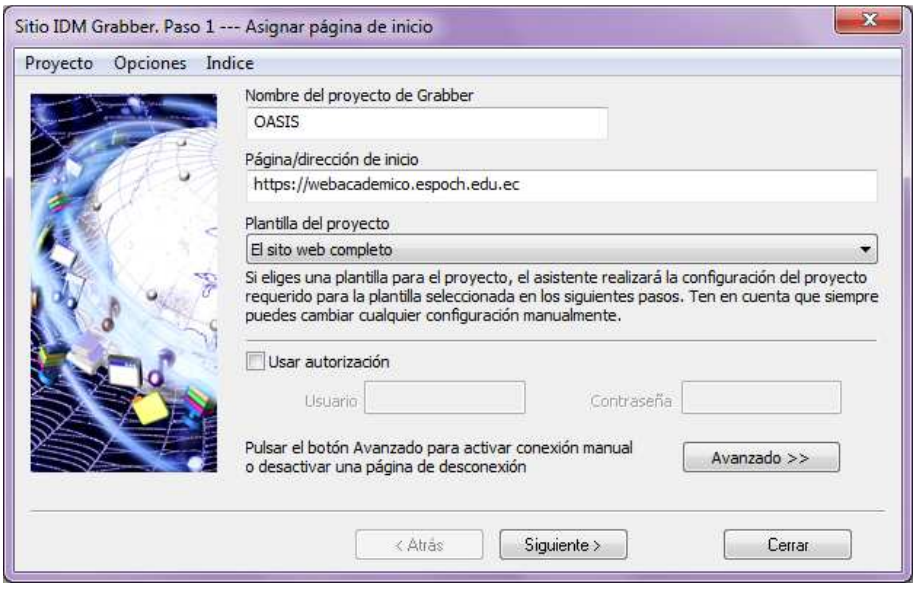
ANEXO 2

CLONACIÓN DEL SITIO WEB ACADEMICO DE LA ESPOCH OASIS

Para realizar la clonación del sitio web académico se utilizo la herramienta Internet Download Manager 6.05, la figura siguiente es la ventana principal del programa.

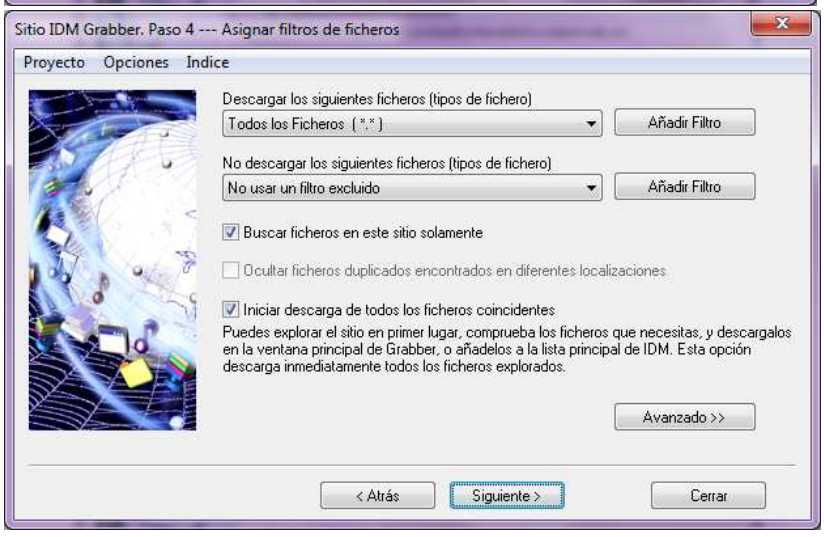


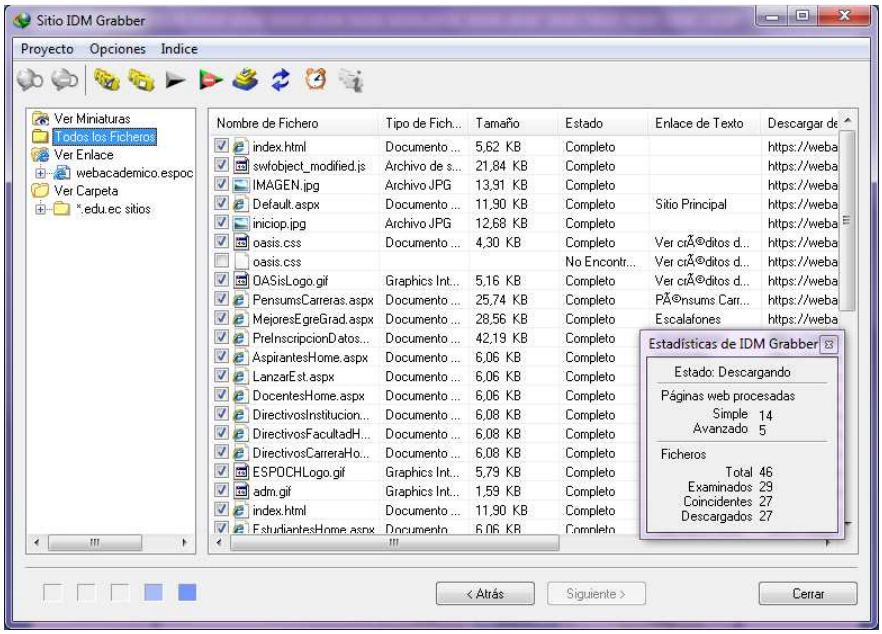
Dar clic en la opción Graber de la barra de herramientas para iniciar la clonación del sitio web. En la ventana nos pide el nombre del proyecto y seleccione la opción El sitio web completo.

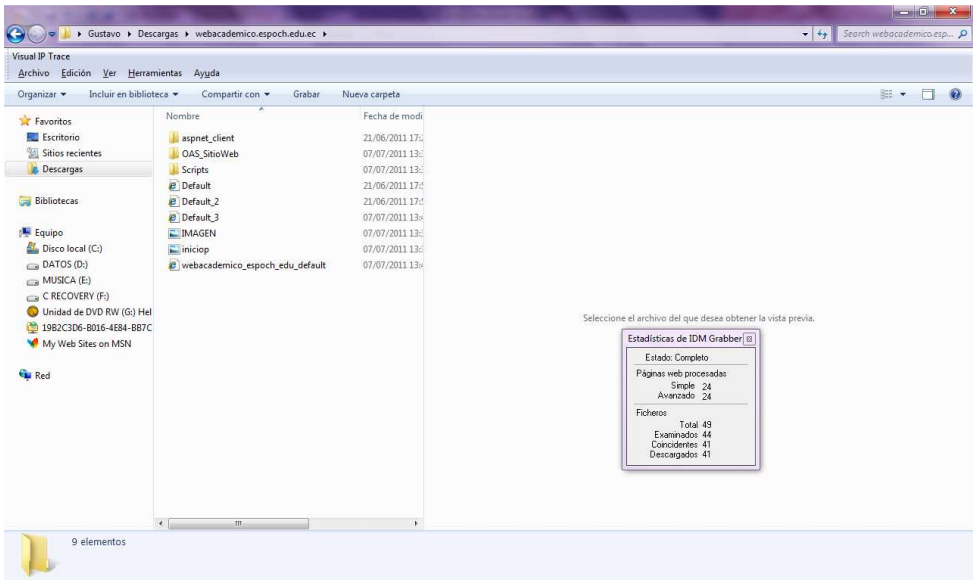


Dar clic en siguiente y en la ventana de dialogo indique la ruta donde desea guardar el proyecto.

En las siguientes pantallas dejar las opciones por defecto y dar clic en el botón siguiente.







Una vez finalizado el proceso debe guardar el proyecto para poder abrirlo posteriormente.

ANEXO 3

OFICIO DE RESTRICIÓN A LA ESCENA DEL CRIMEN

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DEPARTAMENTO DE SISTEMAS Y TELEMÁTICA

Fono: 03- 2998200, ext. 103 e-mail: desitel@espoch.edu.ec
Panamericana Sur Km. 1,5

Riobamba, <<fecha>>

Señores

Técnicos Informáticos y Personal de Apoyo del DESITEL

Presente

Luego de saludarles, les informo que se restringe el acceso al servidor de base de datos del Sistema Académico de forma física como lógica, a las siguientes personas:

a)

b)

……..

Esta decisión se toma debido a que se realizara un Proceso de Análisis Forense en la Base de Datos Oasis luego de ocurrido un incidente que justifica la ejecución de dicho proceso desde <<fecha y hora>> hasta la entrega del informe final.

La restricción de acceso deberá ser acatada inmediatamente luego de la recepción de este oficio, caso contrario se sancionará a la persona o personas que no acaten esta disposición, de acuerdo al reglamento interno institucional.

Se informa además que durante el periodo que tome el proceso de análisis forense se deberá documentar los accesos al Datacenter, cuando se deba realizar operaciones que permitan garantizar el correcto funcionamiento del resto de aplicaciones o servicios de red, esto con el objetivo de facilitar y garantizar las actividades del proceso de análisis forense

Atentamente:

Dr. Carlos Buenaño
DIRECTOR DE DESITEL

ANEXO 4

AUTORIZACIÓN PARA ANÁLISIS FORENSE

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DEPARTAMENTO DE SISTEMAS Y TELEMÁTICA

Fono: 03- 2998200, ext. 103 e-mail: desitel@espoch.edu.ec
Panamericana Sur Km. 1,5

Riobamba, <<fecha>>

Señores

Técnicos Informáticos y Personal de Apoyo del DESITEL

Presente

Luego de saludarles, les informo que se autoriza se realice un Proceso de Análisis Forense en la Base de Datos del Sistema Académico Oasis, a <<Analista Forense 1>>, <<Analista Forense 2>>, …. <<Analista Forense N>>; luego de ocurrido un incidente que justifica la ejecución de dicho proceso desde <<fecha y hora>> hasta la entrega del informe final.

Se informa además que durante el periodo que tome el proceso de análisis forense se deberá documentar los accesos al Datacenter, cuando se deba realizar operaciones que permitan garantizar el correcto funcionamiento del resto de aplicaciones o servicios de red, esto con el objetivo de facilitar y garantizar las actividades del proceso de análisis forense

Atentamente:

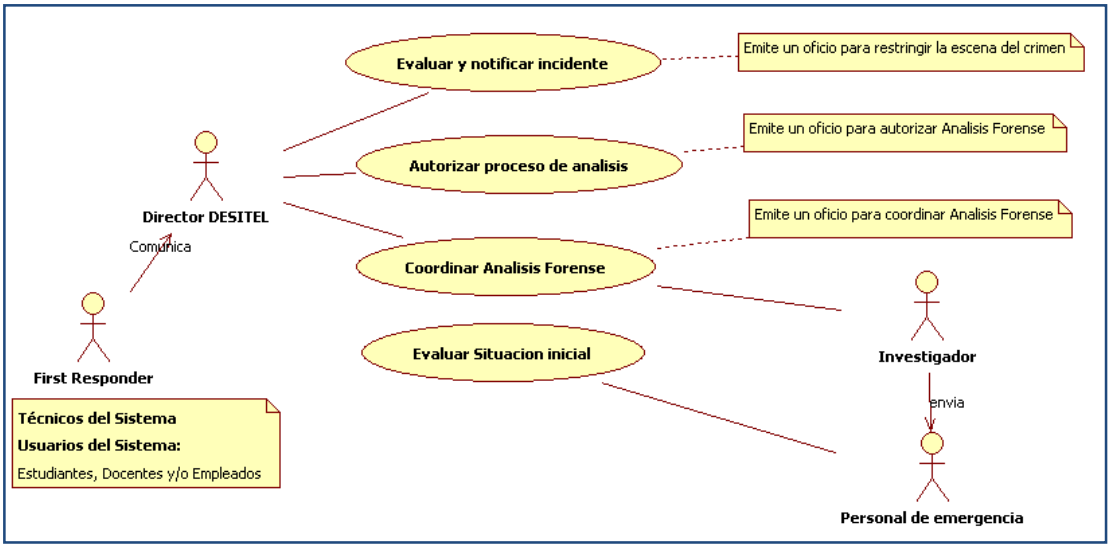
Dr. Carlos Buenaño

DIRECTOR DE DESITEL

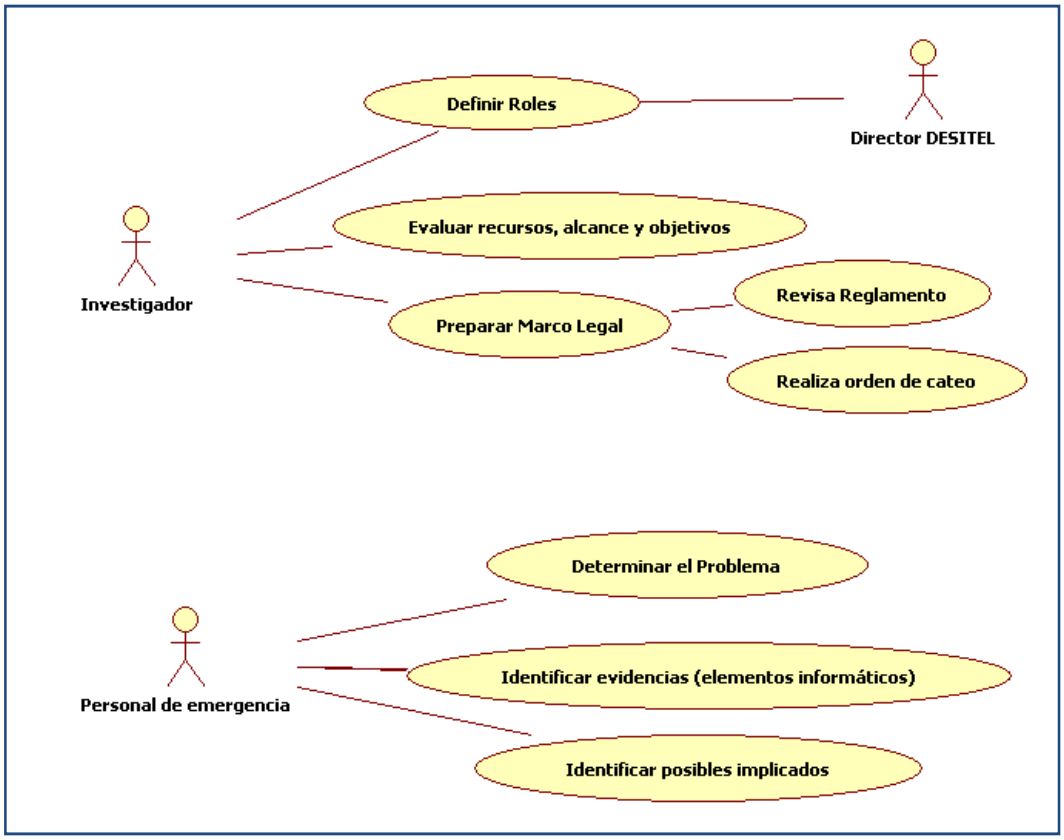
ANEXO 5

DIAGRAMAS DECASOS DE USO DE ACUERDO A ROLES

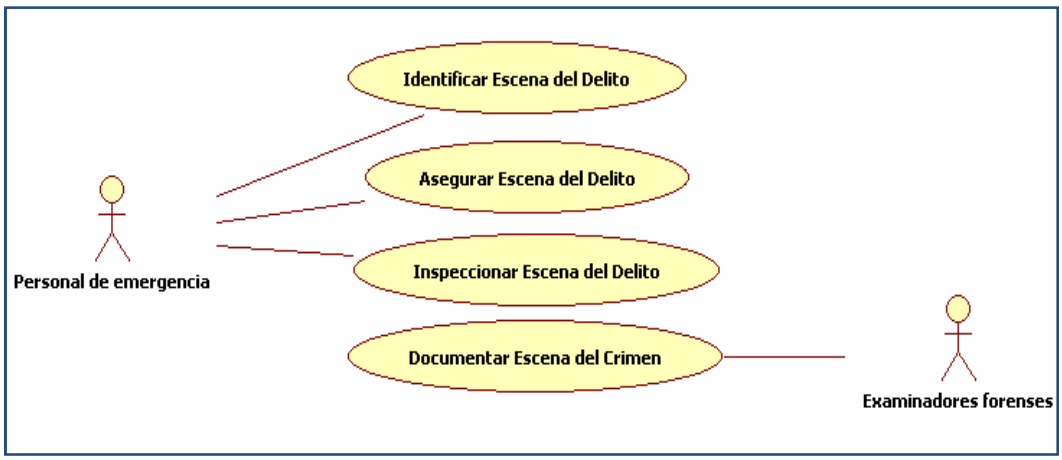
Diagramas de Caso de Uso: Evaluar y Autorizar proceso de Análisis Forense



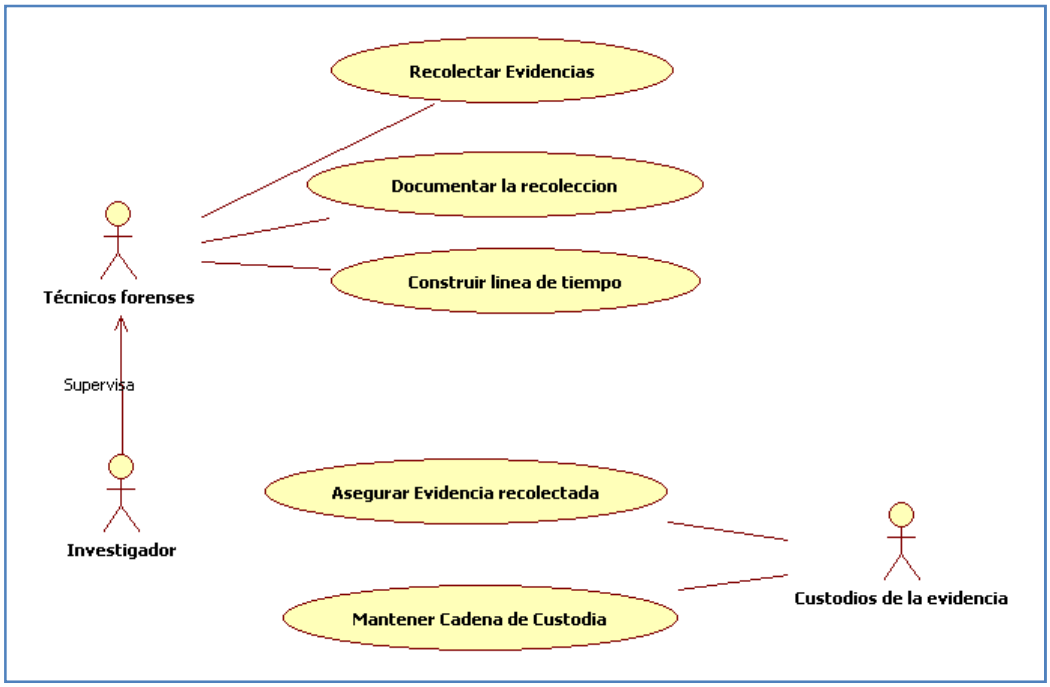
Diagramas de Casos de Uso Fase 1: Planificar proceso de Análisis Forense



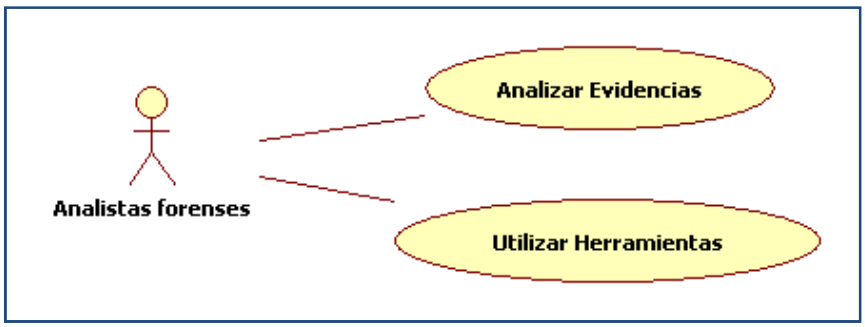
Diagramas de Casos de Uso Fase 2: Verificar proceso de Análisis Forense



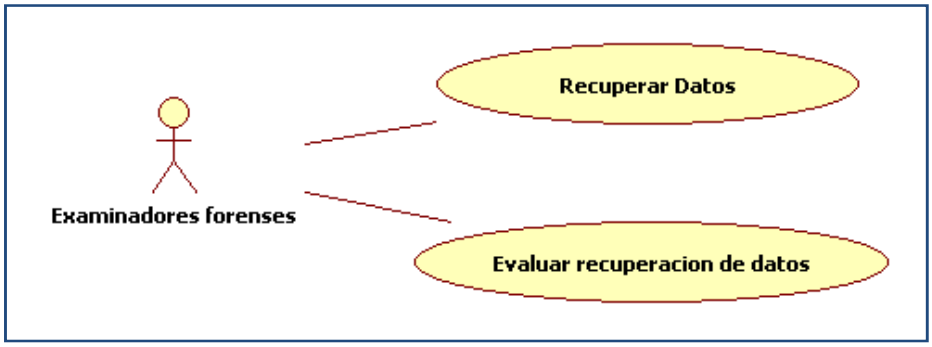
Diagramas de Casos de Uso Fase 3: Recolectar Evidencia para proceso de Análisis Forense



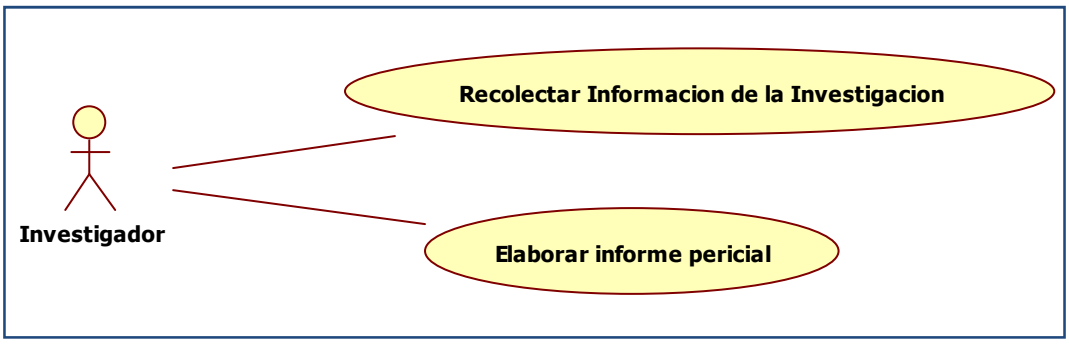
Diagramas de Casos de Uso Fase 4: Analizar Evidencias



Diagramas de Casos de Uso Fase 5: Recuperar datos

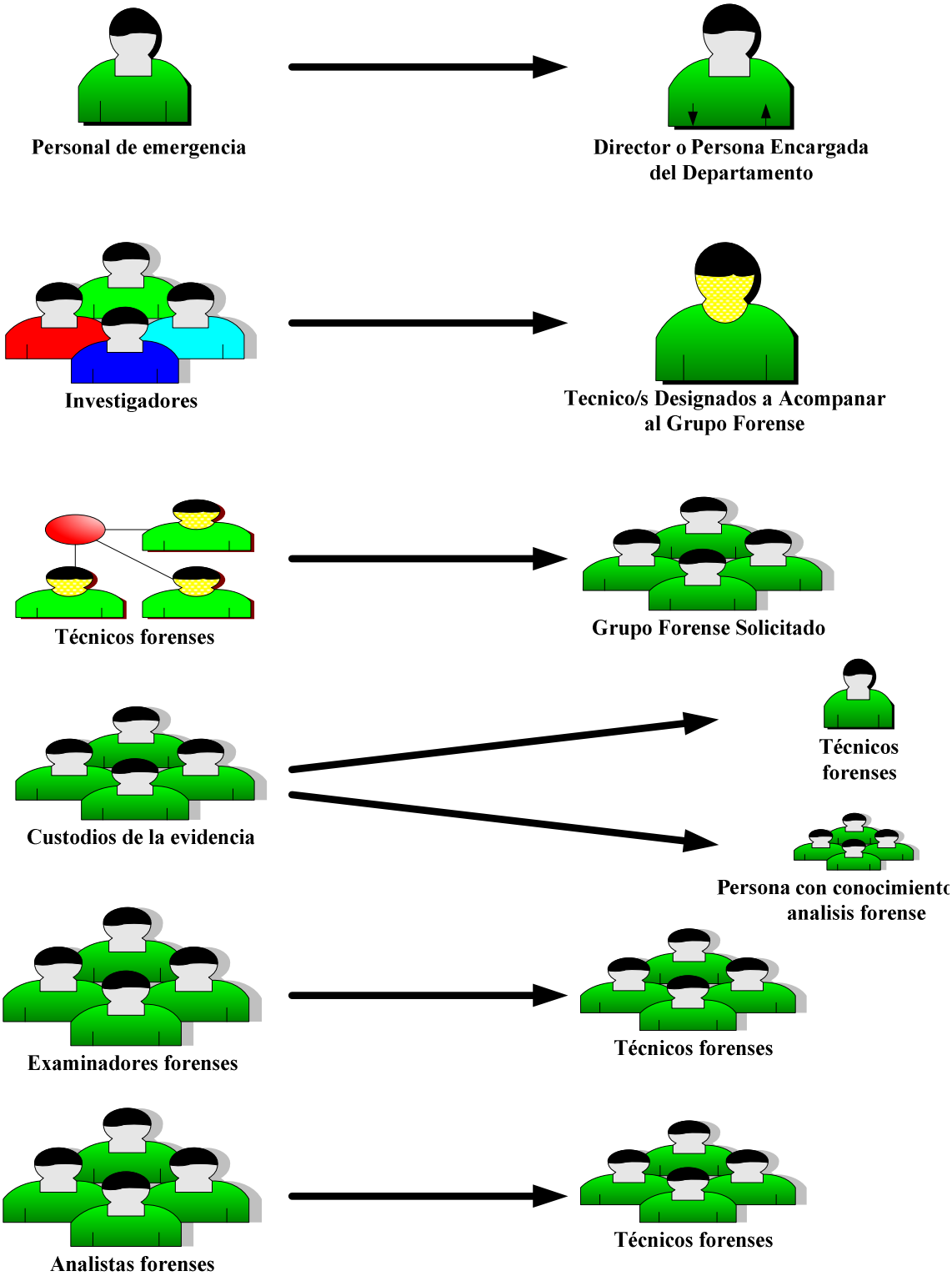


Diagramas de Casos de Uso de la Fase 6: Presentar Informe



ANEXO 6

DEFINICIÓN DE ROLES



Personal de emergencia: Director o Persona Encargada del Departamento De Sistemas y Telemática es quien evalúa la situación, dentro de sus responsabilidades tenemos: solicitar una persona que acompañe al grupo forense y convocar al personal apropiado para el soporte requerido

Investigadores: Es la persona o personas que supersisan al grupo forense, los investigadores son personas con conocimiento de la plataforma, sentencias SQL, etc, los mismos que no deben ser parte del grupo que va ser analizado como escena del incidente.

Técnicos forenses: son las personas que tienen conocimiento sobre análisis forense, utilización de herramientas y procedimientos forenses.

Custodios de la evidencia: puede estar a cargo de los mismos técnicos forenses u otras personas que tengan conocimientos de análisis forense.

Examinadores forenses: puede estar a cargo de los mismos técnicos forenses u otras personas que tengan conocimientos de análisis forense pero. Generalmente no es recomendable tener personas que tengan los roles de técnicos y examinadores al mismo tiempo.

Analistas forenses: puede estar a cargo de los mismos técnicos forenses u otras personas que tengan conocimientos de análisis forense.

ANEXO 7

OFICIO PARA COORDINAR ANÁLISIS FORENSE

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DEPARTAMENTO DE SISTEMAS Y TELEMÁTICA

Fono: 03- 2998200, ext. 103 e-mail: desitel@espoch.edu.ec
Panamericana Sur Km. 1,5

Riobamba, <<Fecha>>

<<Titulo>>

<<Nombre Coordinador>>

<<Cargo>>

Presente.

Luego de saludarle, a partir de <<fecha y hora>> designo a usted como <<Investigador>> para que acompañe, apoye y garantice la ejecución de las actividades a realizar por parte del equipo forense, comprometiendo fundamentalmente su designación a vigilar que todas las actividades de investigación forense se realicen única y estrictamente sobre el ámbito de investigación definido.

Atentamente,

DR. Carlos Buenaño

DIRECTOR DE DESITEL

ANEXO 8

REGLAMENTO DE DESITEL

(Ver en CD)

ANEXO 9

ORDEN DE CATEO

(Ver en CD)

ANEXO 10

FORMULARIO DE REGISTROS DE EVIDENCIA DE LA COMPUTADORA

Almacenamiento secundario fijo y removible

Cantidad	Tipo De Disquetera- CD-ROM-DVD-DISCO Rigido-IDE-SCSI-USB-ZIP-JAZZ-PENDRIVE	Marca/Modelo	Velocidad/Capacidad	Nro. Serie

Accesorios y Periféricos

Cantidad	Tipo Placa de Red-Modem-cámara-tarjeta de acceso-impresora, etc.	Marca/Modelo	Velocidad/Capacidad	Nro. Serie

Firma de los peritos responsables_____

_____

FORMULARIO DE REGISTROS DE EVIDENCIA DE LA COMPUTADORA

Fecha: _____

Lugar: _____

Caso: _____

Juzgado _____

Perito/s Responsable/s:

_____

_____

Especificaciones de la computadora

Marca	Modelo	Nro de serie	Placa Madre (Marca/Modelo)	Microprocesador (Marca/Modelo)	Memoria Ram	Memoria Cache

Firma de los peritos responsables_____

_____

ANEXO 11

FORMULARIO DE RESULTADO DE EVIDENCIAS

Fecha: _____

Caso: _____

Perito/s Responsable/s:

_____

_____

Número de Componente ☐

Número de identificación	Responsable maneja la evidencia	Cargo	Tipo de Delito	Nombre de la Evidencia	Software empleado	Resultado (A/N)	Tiempo de Descubrirla

Firma de los peritos responsables_____

_____

ANEXO 12

FORMULARIO DE ESTADO DE EVIDENCIAS

Fecha: _____

Hora: _____

Caso: _____

Perito/s Responsable/s: _____

_____

Número de Evidencia ☐

Número de identificación	Responsable maneja la evidencia	Código Evidencia	Nombre Evidencia	Copia de la Evidencia(s/n)	Donde se mantiene la original

Firma de los peritos responsables_____

_____

ANEXO 13

Como antecedente se puede mencionar que el DataCenter donde se encuentra el Servidor que aloja la Base de Datos OASIS cuentas con seguridades como el control de ingreso; mediante la digitación de un código secreto (que posee cada técnico de DESITEL) y cámaras de seguridad que graban el ingreso y salida del personal al DataCenter.

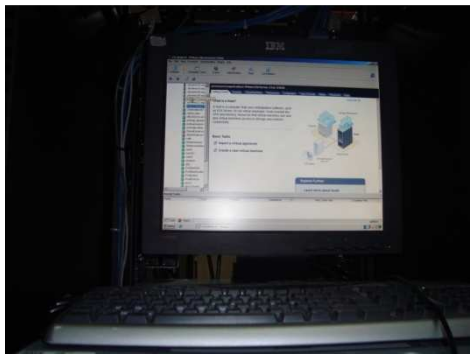
Call Center

Cámara de seguridad

Blasers

Servidores

Servidores con tecnología HP



Pantalla inicial del S.O donde esta OASIS

Array de Discos

Blasers

Procesador HP

Vista de Servidores de DESITEL

Sensor en el DataCenter

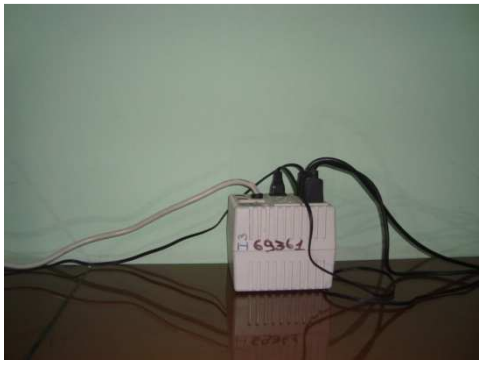
Puerta de Ingreso al Data Center

Área de Desarrollo

Técnicos de DESITEL

CPU afectado

Pantalla de equipo victima



Regulador

Parte trasera del CPU victima

ANEXO 14

TABLA DE VALORACIÓN DE DETECCIÓN DE VULNERABILIDADES DE ACUERDO A RANGOS

Rangos	Valoración
100%-70%	ALTO
69%-50%	MEDIO
49%-0%	BAJO

DETECCION DE VULNERABILIDADES EN SQL SERVER 2005 Y MySQL 5.X

VULNERABILIDADES	PROMEDIO (%)		TOTAL (%)	Valoración
	SERVER 2005	MySQL 5.X		
Inyección SQL	66.67%	100%	83.34%	ALTO
Puertos Abiertos	100%	100%	100%	ALTO
Contraseñas débiles	66.67%	50%	58.34%	MEDIO
Acceso a elementos de la BD (tablas, procedimientos, vistas, etc.)	66.67%	100%	83.34%	ALTO
Otros (Framework, Memoria, etc)	83.33%	100%	91.67%	ALTO

BIBLIOGRAFÍA

(1) A DIGITAL FORENSIC INVESTIGATIVE MODEL FOR BUSINESS ORGANISATIONS [en línea] <http://icsa.cs.up.ac.za/issa/2006/Proceedings/Research/57_Paper.pdf > 2010 -01- 04

(2) ALMACENAMIENTO MYSQL [en línea] <http://translate.google.com.ec/translate?hl=es&langpair=en%7Ces&u=http://dev.mysql.com/doc/refman/5.0/en/storage-requirements.html> 2009 - 01- 21

(3) ANÁLISIS FORENSE DIGITAL [en línea] <http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf> 2009- 10- 23

(4) AUTORIZACIÓN Y PERMISOS EN SQL SERVER (ADO.NET) [En línea] <http://msdn.microsoft.com/es-es/library/bb669084.aspx> 2009-12- 21

(5) BUENAS PRÁCTICAS EN LA ADMINISTRACIÓN DE LA EVIDENCIA DIGITAL [en línea], <http://profesores.is.escuelaing.edu.co/asignaturas/sypi20071/FOLLETOS%20Y%20MATERIAL%20DE%20ESTUDIO/forense/buenas%2520practica%2520evidencia%2520digital%2520jcano.pdf> 2010- 01- 04

(6) BUFFER OVERFLOW [en línea] <http://www.owasp.org/index.php/Buffer_Overflow> 2010-02-10

(7) COMPUTO FORENSE [en línea] <http://es.wikipedia.org/wiki/C%C3%B3mputo_forense>2009-11- 23

(8) CREACIÓN DE USUARIOS Y ADMINISTRACIÓN DE PRIVILEGIOS [en línea] <http://www.udb.edu.sv/Academia/Laboratorios/informatica/SQLServer/guia5SQLS.pdf> 2009-12- 21

(9) CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA [en línea] <http://materias.fi.uba.ar/6669/alumnos/2007-1/Informatica%20Forense%20-%G3.pdf > 2009- 12 -21

(10) CROSS XXS [en línea]

< http://advanced-rar-password-recovery.softonic.com/>
2009- 01- 21

(11) CURSO SOBRE DELITOS INFORMÁTICOS [en línea] <http://curso-sobre-delitos-informticos-1221967231432923-8.ppt> 2009- 10- 21

(12) DELITOS INFORMÁTICOS [en línea] <http://www.derechoecuador.com/index.php?option=com_content&task=view&id=3925&Itemid=426> 2009 -10 -23

(13) DETECTANDO ROOTKITS LINUX [en línea] <http://www.uned.es/csi/sistemas/secure/seguridad/docs/rootkitlin.htm> 2010- 02- 10

(14) ELECTRONIC CRIME SCENE INVESTIGACIÓN [en línea], <http://www.ncjrs.gov/pdffiles1/nij/187736.pdf > 2010- 01- 04

(15) ENCRIPCIÓN DE DATOS CON SQL SERVER 2005 [en línea] <http://gerardoramosun.wordpress.com/2007/04/29/encripción-de-datos-con-sql-server-2005/> 2010-02-10

(16) GUIDE TO INTEGRATING FORENSICS INTO INCIDENT RESPONSE [en línea] <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf> 2010- 01- 05

(17) INFORMÁTICA FORENSE: GENERALIDADES, ASPECTOS TÉCNICOS Y HERRAMIENTAS [en línea] <http://w ww.criptored.upm.es/guiateoria> 2009-10-21

(18) INTEGRIDAD Y SEGURIDAD EN LOS SISTEMAS DE BASES DE DATOS [en línea] <http://alfa.facyt.uc.edu.ve/computación/pensum/cs0347/download/exposiciónes2005-2006/Integridad%20y%20Seguridad.pdf> 2009- 10- 21

(19) INTRODUCCIÓN A LA INFORMÁTICA FORENSE [en línea] <http://www.acis.org.co/fileadmin/Revista_96/dos.pdf> 2009-10-23

(20) INYECCIÓN SQL EN MICROSOFT SQL SERVER [en línea] < http://jbyte-security.blogspot.com/2009/06/inyección-sql-en-microsoft-sql-server.html> 2010- 02- 10

(21) LOS "ROOTKIT" AMENAZAS INVISIBLES Y DESTRUCTIVAS DE LOS SISTEMAS OPERATIVOS [en línea] < http://persystems.net/sosvirus/pregunta/rootkit.htm > 2010-12-21

(22) MODULO 5 [en línea] < http://www.rodrigosalinas.cl/wp-content/uploads/2008/01/Seguridad/Modulo5.ppt> 2009- 12- 21

(23) PERFIL SOBRE LOS DELITOS INFORMÁTICOS EN EL ECUADOR [en línea] < http://www.criptored.upm.es/guiateoria/gt_m592d.htm> 2010- 02 -10

(24) ROOTKIT [en línea] < http://es.wikipedia.org/wiki/RootkitRootkit> 2009 -02- 17

(25) SEGURIDAD EN BASE DE DATOS [en línea] <www.hernanracciatti.com.ar/.../HPP26_Seguridad_en_Base_de_Datos.pdf > 2010-01-21

(26) SQL [en línea] <http://en.wikipedia.org/wiki/Relational_database_management_system> 2009 -12- 21

(27) TECHNET: INTRODUCCIÓN A MICROSOFT OPERATIONS MANAGER 2005 [en línea] <download.microsoft.com/download/0/9/e/.../analisis_forense.ppt> 2009- 01- 03