**CIS0910SD03**

# Guía metodológica para identificar y validar la aplicación de técnicas anti-forenses en equipos con sistema operativo Windows XP Service Pack 3.

**ARMANDO BOTERO VILLA**
**IVAN FELIPE CAMERO PADILLA**

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERIA
CARRERA DE INGENIERIA DE SISTEMAS
BOGOTÁ, D.C.
2010
CIS0910SD03

# Guía metodológica para identificar y validar la aplicación de técnicas anti-forenses en equipos con sistema operativo Windows XP Service Pack 3.

**http://pegasus.javeriana.edu.co/~CIS0910SD03/**

**Autores:**
Armando Botero Villa
Iván Felipe Camero Padilla

MEMORIA DEL TRABAJO DE GRADO REALIZADO PARA CUMPLIR UNO DE LOS REQUISITOS PARA OPTAR AL TITULO DE INGENIERO DE SISTEMAS

**Director**

Jeimy Cano Martínez

**Jurados del Trabajo de Grado**

Edgar Enrique Ruíz

Fabián Contreras

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERIA
CARRERA DE INGENIERIA DE SISTEMAS
BOGOTÁ, D.C.
Diciembre, 2010

**PONTIFICIA UNIVERSIDAD JAVERIANA**
**FACULTAD DE INGENIERIA**
**CARRERA DE INGENIERIA DE SISTEMAS**

**Rector Magnífico**
Joaquín Emilio Sánchez García S.J.
**Decano Académico Facultad de Ingeniería**
Ingeniero Francisco Javier Rebolledo Muñoz
**Decano del Medio Universitario Facultad de Ingeniería**
Padre Sergio Bernal Restrepo S.J.
**Directora de la Carrera de Ingeniería de Sistemas**
Ingeniero Luis Carlos Díaz Chaparro
**Director Departamento de Ingeniería de Sistemas**
Ingeniero César Julio Bustacara Medina

**Nota de Aceptación**

_____

_____

_____

_____

_____

Jeimy José Cano Martínez

**Director del Proyecto**

_____

**Edgar Enrique Ruíz**

**Jurado**

_____

**Fabián Contreras**

**Jurado**

### Artículo 23 de la Resolución No. 1 de Junio de 1946

*"La Universidad no se hace responsable de los conceptos emitidos por sus alumnos en sus proyectos de grado. Sólo velará porque no se publique nada contrario al dogma y la moral católica y porque no contengan ataques o polémicas puramente personales. Antes bien, que se vean en ellos el anhelo de buscar la verdad y la Justicia"*

# TABLA DE CONTENIDO

# ÍNDICE DE ILUSTRACIONES

# ÍNDICE DE TABLAS

# ABSTRACT

Nowadays, due to the growth and the appearance of new information technologies, new gaps in security have opened allowing to harm in the integrity, privacy and availability of the information assets owned by any kind of organization; in addition to this, the increase of the development of new software that allows the attacker to make its job easier, permitting him to destroy, hide, eliminate or counterfeit the sources of evidence that could have been left while he was working. Hence, this work proposes a methodology by which a forensic investigator can identify traces that help him conclude the use of an anti-forensic technique in a cybercrime that involves a computer with a Microsoft Windows XP Service Pack 3 operating system installed.

# RESUMEN

En la actualidad, debido al crecimiento y aparición de nuevas tecnologías de información, se ha dado paso a nuevas brechas de seguridad por medio de las cuales se ve afectada la integridad, confidencialidad y disponibilidad de los activos de información pertenecientes a cualquier tipo de organización; adicionalmente, se ha incrementado el desarrollo de herramientas que facilitan la ejecución de delitos informáticos, permitiéndole a un atacante ocultar, falsificar, eliminar o destruir las fuentes de evidencia que pudo haber dejado durante sus labores delictivas. Por lo tanto, el presente trabajo de grado propone una metodología por medio de la cual un investigador forense estaría en capacidad de identificar rastros que ayuden a concluir el uso de técnicas anti-forenses en un delito informático, en el cual se vea comprometido algún dispositivo con sistema operativo Microsoft Windows XP con Service Pack 3 instalado.

# INTRODUCCIÓN

En la actualidad se cuenta con una tecnología de la información avanzada y con un nivel de maduración cada vez mayor, introducida a fondo en la vida de las organizaciones y personas, lo que ha generado que la información se convierta en un bien de vital importancia; que debe ser protegido de amenazas que puedan dañarlo, robarlo, modificarlo, o incluso aprovecharlo para múltiples acciones mal intencionadas o ilícitas.

La evolución de los sistemas computacionales ha generado un incremento en las vulnerabilidades, las cuales han sido aprovechadas al máximo por los atacantes o intrusos. Una muestra de las distintas formas de explotar estas vulnerabilidades se puede encontrar en la siguiente ilustración, que evidencia cómo los atacantes desarrollan y refinan cada vez más sus técnicas, para sacar provecho de los problemas inherentes de las nuevas tecnologías [12].

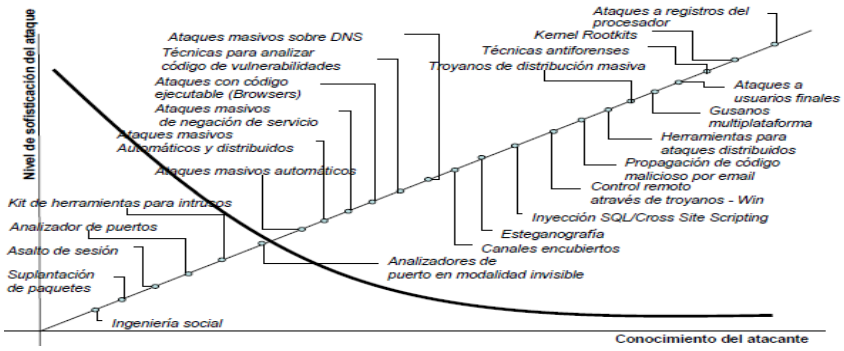


Ilustración 1 Clasificación ataques [12]

Cómo muestra la imagen, a medida que los conocimientos de los atacantes aumentan, se incrementa proporcionalmente el nivel de sofisticación de los ataques. Esto revela que hoy en día, las organizaciones y los directores de los departamentos de seguridad, no se están enfrentado a personas inexpertas e ingenuas que solo quieren jugar; se están enfrentando a mentes "*inquietas*" que siempre van más allá de lo que cualquier manual de computación les pueda aportar; estas personas tienen algo que la industria de seguridad informática no tiene: suficiente tiempo y esfuerzo para encontrar alternativas creativas para vulnerar los sistemas [11].

De acuerdo a lo anterior, donde las mentes inquietas poseen distintas motivaciones y la información es un bien sumamente importante en las organizaciones, cualquier ataque podría ser considerado un delito. Por lo tanto, para poder judicializar y presentar los distintos casos a las autoridades judiciales, surge de la criminalística, una nueva disciplina que utiliza un conjunto de herramientas, estrategias y acciones para descubrir en medios informáticos, la evidencia digital que respalde y compruebe cualquier acusación frente a la investigación de un delito informático [11].

Ésta disciplina se conoce como Informática Forense, la cual según el FBI[1] se define como la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional [50]. Sus principales objetivos son [34]:

1. La compensación de los daños causados por los criminales o intrusos.

2. La persecución y procesamiento judicial de los criminales.

3. La creación y aplicación de medidas para prevenir casos similares.

Detallando el segundo objetivo de la informática forense, "*La persecución y procesamiento judicial de los criminales*", éste tiene como eje central la evidencia digital, para la investigación y una eventual judicialización de los implicados en el caso de estudio.

En esta dirección la evidencia digital se define como cualquier registro generado o almacenado en un sistema computacional que puede ser utilizado como elemento material probatorio en un proceso legal [11].

De esta manera, la evidencia digital puede ser dividida en tres categorías [60]:

a) Registros almacenados en el equipo de tecnología informática; por ejemplo correo electrónicos, archivos de aplicaciones de ofimática, imágenes, etc.
b) Registros generados por los equipos de tecnología informática; por ejemplo registros de auditoría, registros de transacciones, registros de eventos, etc.

[1] Federal Bureau of Investigation

c) Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática; por ejemplo hojas de cálculo financieras, consultas especializadas en bases de datos, vistas parciales de datos, etc.

Adicionalmente, la evidencia digital posee unas características especiales que además de diferenciarla de la evidencia física, la convierten en un constante reto para los investigadores de informática forense. Éstas características son las siguientes [11]:

- Es volátil
- Es anónima
- Es duplicable
- Es alterable y modificable
- Es eliminable

Si se parte del hecho que los intrusos basan sus ataques en conocimientos avanzados en informática forense, en las propiedades de la evidencia digital y apoyándose de la frase planteada por Simple Nomad 2006 "*Si controlamos los bits y bytes, y además conocemos como funcionan las herramientas Forenses, podemos controlar la dirección de la investigación forense*", se podría decir que la unión de estas tres últimas premisas, define a grandes rasgos "*las técnicas anti-forenses*".

# 1. DESCRIPCIÓN GENERAL DEL TRABAJO DE GRADO

## 1.1 Formulación

Actualmente, la informática forense cuenta con protocolos que formalmente describen cómo se debe llevar a cabo una investigación con el único fin de entregar resultados concretos que pongan de manifiesto el quién, el cómo, el dónde, el cuándo, el para qué, el con qué y el porqué de un hecho. Estos protocolos son definidos por las unidades especializadas en delitos informáticos de cada país, basándose en modelos y buenas prácticas, en propuestas del IOCE (International Organization on Computer Evidence) [11] en lo que el departamento de justicia de los Estados Unidos plantea en su "Guide for First Responders", etc. [31]. Sin embargo, en estos protocolos, no se contempla la aplicación de técnicas anti-forenses (cualquier intento exitoso efectuado por un individuo o proceso que impacte de manera negativa la identificación, la disponibilidad, la confiabilidad y la relevancia de la evidencia digital en un proceso forense)" [11], en la ejecución del ataque.

La mayoría de los ataques estudiados por la informática forense se observan a nivel de empresas que utilizan el sistema operativo Windows XP, el cual hoy por hoy es la versión más estable y segura de Windows [77]. Es de resaltar, que el auge de Windows XP promovió el estudio de la plataforma; estudio que concluyó en aspectos positivos para Microsoft y negativos para sus usuarios. Entre los aspectos negativos, se cita el hecho de permitirle a los atacantes evaluar cuáles son sus vulnerabilidades y atacarlo por ahí; y entre los positivos , permitirle a Microsoft realizar procesos de reingeniería a su sistema operativo al analizar las deficiencias encontradas por los atacantes. Esto impulsó el lanzamiento de diferentes *service packs con* los cuales se iba mejorando la estabilidad y seguridad del sistema operativo, en tres versiones progresivas, siendo la última, la más refinada de todas. Durante éste proceso, se encontraron varias falencias en la seguridad de Windows XP que terminaron por convertirse en oportunidades de ataques para los criminales digitales.

Al adquirir conocimientos sobre las vulnerabilidades de Windows, un criminal puede aplicar diferentes métodos y técnicas para mimetizar, manipular, deshabilitar o destruir [27] evidencia digital con el objetivo de agravar o desviar una investigación. Es por esto que surge

la necesidad de incorporar a los manuales que guían las investigaciones de informática forense, un protocolo que identifique la aplicación de técnicas anti-forenses en un crimen digital.

En este contexto, el presente documento busca responder al siguiente interrogante: *¿Cómo identificar y validar la presencia de una técnica anti-forense en el análisis de información en un computador que contenga un sistema de archivos NTFS bajo el sistema operativo Windows XP SP3, encontrado en una escena del crimen?*

## 1.2 Justificación

En informática forense existen distintos protocolos a seguir en una investigación, que buscan definir procesos confiables y que garanticen resultados válidos y suficientes para aplicar algún tipo de acción legal. Estos protocolos se basan en un conjunto de buenas prácticas acordadas por diferentes organizaciones y entidades gubernamentales, en donde son ajustados a necesidades particulares para la construcción de los procesos de cómputo forenses.

Aunque las diferentes metodologías de investigación forense han sido probadas en distintos escenarios que han logrado demostrar su correcto funcionamiento, surgieron una serie de técnicas que permiten burlar los procesos forenses, con lo que es posible evitar que se descubran evidencias, rastros, autores u objetivo del ataque.

Debido al surgimiento de estas técnicas llamadas Anti-forenses, se vulnera la confiabilidad de los resultados arrojados por los protocolos de investigación, ya que actualmente estos no cuentan con procesos que evalúen si en el ataque está involucrada alguna técnica anti-forenses. Por consecuencia, no se es posible ser concluyente en las afirmaciones después de la investigación, puesto que no se puede asegurar no estar llegando a una conclusión construida por el mismo atacante, por ejemplo, el incriminar a otra persona u organización.

Por tal motivo, este documento establece un conjunto de elementos conceptuales y aplicados para incorporar en los protocolos de investigación de informática forense un proceso que evalué si en un ataque se aplicó alguna técnica anti-forense. Como resultado para este trabajo se generará una guía metodológica en donde se detalla cómo realizar la validación de

aplicación de técnicas anti-forenses en máquinas que utilicen sistemas operativos Windows XP Service Pack 3.

## 1.3 Objetivo general

Desarrollar una guía metodológica para identificar y evidenciar la aplicación de técnicas anti-forenses en el análisis de información en un computador que contenga un sistema de archivos NTFS bajo el sistema operativo Windows XP SP3, encontrado en una escena del crimen.

## 1.4 Objetivos específicos

1. Estudiar y analizar el estado del arte de la criminalística, la criminalística en medios informáticos y las técnicas anti-forenses existentes, enfocando estas últimas al sistema operativo Windows XP SP3 y en el funcionamiento del sistema de archivos NTFS.
2. Realizar el diseño de la guía metodológica orientada a la identificación y validación del uso de técnicas anti-forenses en el análisis de la información en computadores con sistemas de archivos NTFS bajo un sistema operativo Windows XP SP3 encontrado en una escena de crimen.
3. Probar y ajustar el diseño de la guía metodológica, basándose en los niveles del Modelo conceptual de Detección y Rastreo de Técnicas Anti-forenses (MoDeRaTA) en un sistema de archivos NFTS en un sistema operativo Windows XP SP3.

# 2. REVISIÓN DE LITERATURA

## 2.1. Fundamentos Forenses

### *2.1.1. Criminalística*

La criminalística es una disciplina que junta todos los estudios relativos a la técnica del crimen, razón por la que puede ser considerada como una ciencia con objeto y métodos propios [26].

A diferencia de la criminología que se ocupa de averiguar por qué una persona realizó un delito, la criminalística ayuda a esclarecer cómo y quién llevo a cabo el delito valiéndose del estudio de los hechos físicos y de las evidencias para reconstruirlo y confirmar una hipótesis.

En una definición más global, las ciencias forenses son la aplicación de la ciencia al derecho. [59] Sin embargo, para llegar a dicha afirmación, fue necesario que se presentara un proceso histórico que no se puede ignorar.

A principios del siglo XVIII policías europeos contrataban a ex delincuentes para que ayudaran desde su conocimiento de "evitación de la detección de delitos y su autor" a esclarecer quién había perpetrado el delito investigado. Un célebre ejemplo de ello fue Vidocq, quien en 1809 fue vinculado por el cuerpo de policía francesa como ayudante y posteriormente fundó en 1825 una red de ex presidiarios llamada la *Sureté*, seguridad en francés, dedicada a la investigación privada. Sus publicaciones sirvieron de base a los conocidos novelistas y paradójicamente estos últimos contribuyeron luego a las metodologías policiales de la época, haciendo evidente que los análisis se hacían de manera subjetiva, casi fantástica. [26]

Fue en 1893 que en su publicación "El manual del juez", el juez de instrucción austriaco, Hans Gross, definió la criminalística como la disciplina que se ha ido desarrollando para descubrir el crimen y el accionar de los delincuentes para evitar la reconstrucción de aquel y su detección. En el mismo, logró reunir todos los conocimientos científicos y técnicos que en su época se aplicaban en la investigación criminal. Gross es reconocido en la materia por nutrir la investigación con los contenidos de campos científicos como la microscopia,

química, física, mineralogía, zoología, botánica, antropometría y las huellas [59]. Relevante en tanto cada una de estas materias se enriquecería del legado de la revolución industrial, lo que le permitiría a la criminalística ser más precisa en sus investigaciones.

Años más tarde, luego de la Segunda Guerra Mundial, la ciencia forense se vio renovada una vez más, producto de los avances tecnológicos de los , distintos campos científicos en tanto: "la epistemología y razonabilidad de la criminalística depende de cada ciencia, arte u oficio, según su pertinencia y conducencia, determinada por la naturaleza de la conducta investigada [26].

En este contexto, la criminalística puede dividirse en tres periodos históricos a saber: la época pre científica, la época científica y la época después de la Segunda Guerra Mundial.

La criminalística general tiene por objetivo capacitar a la persona que vayan a trabajar en la gestión de equipos de trabajo con especialidad requerida, el aporte de soluciones al fenómeno delictivo y en la transformación de evidencias en materiales probatorios a través del método científico. Lo anterior para dominar conceptos que permitan saber que servicios forenses se requieren, remitir de forma "adecuada" a estudio de los peritos las distintas evidencias e interpretar resultados a través de los puntos de vista de distintas pericias forenses.

En esta dirección, el objetivo de la criminalística es determinar a través de qué ciencia se ha de agrupar y analizar la evidencia para luego convertirla en material probatorio; y el del criminalista, es recrear la escena del crimen a través de la ciencia que elija, para descubrir quién fue el responsable..

La criminalística cuenta con una serie de principios que apuntan a recolectar evidencias materiales basadas en teorías. Un ejemplo al respecto es el del principio del intercambio del criminalista francés Locard, quien aduce que en todo contacto entre dos cuerpos siempre existe una transferencia de material [26].

Para el objeto de estudio del presente documento, es posible adaptar los principios de reconstrucción de hechos o fenómenos, el de probabilidad y el de certeza, pues aunque estos se basen en la interacción de evidencias químicas y físicas, también se pueden adaptar a la resolución de casos virtuales.

Aplicar los métodos criminalísticos requiere, antes que nada, verificar la legislación vigente para asegurarse que su uso no vaya a ir en contravía de la ley. Luego, como cualquier otra ciencia, ésta requiere de un proceso científico que ayude a comprobar o refutar hipótesis en torno a la escena del crimen. Es así como los pasos del método científico son aplicados a la criminalística para esclarecer los hechos. Se encuentra entonces en la cabeza del proceso la observación, luego le sigue la medición y descripción de variables cuantitativas. La medición se hace a través de la comparación y la descripción empieza con las percepciones generales para llegar a las particulares. Finalmente, se ejecuta el experimento mediante un intento por recrearla escena del crimen teniendo en cuenta los supuestos antes trabajados por los criminalistas para dar cuenta de si las cosas sí pudieron darse de la manera que ellos las planteaban.

La criminalística aplicada al proceso penal es de vital importancia, pues en ella descansa la actividad técnica de las evidencias, de los materiales probatorios, e incluso de la experticia técnica en tránsito hacia la transformación en prueba [26].

Se podría decir que el criminalístico participa en el proceso penal acusatorio como un perito, un sujeto del juicio que analiza los sucesos desde su punto de vista objetivo [26].

Se registran peritos desde la época del derecho romano, como es el caso de obstetras y arquitectos. No obstante dentro del derecho canónico, con algunas excepciones, se referían a los peritos también como testigos. Cabe anotar que el testigo a diferencia del perito, es un objeto más del juicio que relata los sucesos desde su punto de vista subjetivo, de acuerdo con sus sentidos. En cambio las opiniones de un perito adquieren valor por cuanto sus criterios pueden ser comprobables o cuentan con el reconocimiento de sus pares en su campo de análisis.

Un perito ha de confirmar, no de deliberar, es por ello que ha de mantenerse parcial sin realizar pruebas inquisitoriales o recaer en la pasividad indolente, siendo consciente sobre que puede comentar. Él debe intervenir con sus conocimientos especializados demostrándolos, y demostrando a la vez, su idoneidad, por medio de títulos profesionales oficiales y experiencia profesional.

De no cumplir con las características antes descritas, resulta recomendable incluir en el proceso a un nuevo perito para asegurar la objetividad de su labor durante el juicio.

Para poder incriminar a un sujeto debe haber relación entre el mismo y la escena del crimen, pues esta última ha de ser el resultado o consecuencia del indiciado.

Fueron filósofos alemanes quienes a principios del siglo XX profundizaron en las teorías de la causalidad contribuyéndole a la materia. Claro está que no basta con apoyarse en las anteriores para establecer las relaciones entre la escena del crimen y el indiciado sino que también, han concluido expertos como Fierro Méndez, resulta importante someter las pruebas e indicios que apuntan en contra del criminal a las teorías de la probabilidad para evitar juicios subjetivos en este ejercicio.

La elaboración de perfiles criminales es una técnica de investigación judicial que consiste en inferir aspectos psicosociales del perpetrador con base en un análisis psicológico, criminalístico y forense de sus crímenes, con el fin de identificar un tipo de persona (no un persona en particular) para orientar la investigación y la captura [26].

Si bien desde el siglo XIX investigadores europeos como Turvey y Lombroso crearon diferentes perfiles para encajar a los distintos criminales, se podría decir que no fue sino hasta casi un siglo después que se empezaron a emplear técnicas de este campo, como el reconocido perfil psicológico de Brussel, desde entonces se ha ido perfeccionando la técnica cada vez más para efectos de ayudar al investigador a delimitar el número de posibles sospechosos. Es así como este puede servirse de: a) perfiles de agresores conocidos, perfil psicológico o método inductivo, que parte de características particulares a generales, de b) perfiles de agresores conocidos, perfil criminal o método deductivo que desde características generales obtiene particulares y del c) perfil geográfico, que corresponde a la escena del crimen.

En un trabajo de grado titulado “Elaboración de perfiles criminales desconocidos con base en la escena del crimen” las autoras Tapias, Avellaneda, Moncada y Pérez consiguieron esbozar una propuesta del proceso de generación de perfiles criminales desconocidos con base en la escena del crimen como su nombre lo indica.

Dividen entonces el proceso en 3 etapas. En la primera es necesario obtener información del contexto sociocultural dónde ocurrió la escena del crimen y a su vez proteger la escena del crimen cercando a la misma. En la segunda, ha de realizarse un análisis a la víctima quien de estar viva podrá ser entrevistada y si no será psicológicamente reconstruida a partir de las declaraciones de testigos que la hayan conocido o visto por última vez, de los lugares que frecuentaba, las actividades que realizaba, incluso la ropa que llevaba el día del crimen. Adicionalmente ha de obtenerse un análisis de la escena que incluya descripciones hipotéticas basadas en la posición de las evidencias allí dejadas para llegar a conclusiones de cómo se perpetró el crimen, sus circunstancias, su ángulo, sus instrumentos, etc. [26]. Cuando la persona encargada de elaborar este perfil cuenta con una enorme experiencia es capaz de clasificar los crímenes con mayor facilidad para saber si se trata de un criminal reincidente o si por el contrario es la primera vez que el sujeto comete un crimen.

Los asesinatos en masa, donde mueren más de cuatro personas, también pueden ser clasificados. El asesinato en masa clásico cuenta con un perpetrador trastornado mentalmente que actúa contra "todos" los que estén en un mismo lugar. En cambio, el asesino en masa familiar, se dedica literalmente a matar a miembros de su familia. Adicional a estos perfiles de asesino múltiple, se encuentra el del asesino itinerante que mata en 2 o más lugares en un periodo corto de tiempo y el del asesino en serie, que a diferencia del anterior espera entre víctima y víctima para preparar todo el crimen y clasificar a las personas a quienes va a hacer daño.

Asimismo, autores como Ressler, Burgess, Homant y Kennedy aportaron otra serie de variables que podían ser incluidas en los perfiles criminales las cuales incluso llegaban a determinar la procedencia del victimario, sus costumbres, sus preferencias, su comportamiento.

Finalmente, la última etapa consiste en la validación del perfil construido, pues al ser emitido se deben presentar en muchos casos sospechosos dentro de los cuales aparecerá el criminal que luego confesará y corroborará el perfil creado para él. Claro está, que en los casos donde el perfil elaborado no contribuya exitosamente a la captura del perpetrador dicho documento podrá ser reevaluado y reutilizado [26].

Para conservar las evidencias físicas e informes obtenidos luego de los diferentes análisis a la escena del crimen se cuenta con la Cadena de Custodia, un registro que indica en qué lugar y con cuál persona se encuentra la evidencia en todo momento [59].

Es necesario proteger las pruebas de daños o alteraciones que invaliden su acción durante el proceso acusatorio. Así pues, las pruebas deben tener empaques y marquillas características que ayuden a preservarlas mejor. Estas marquillas deberán incluir una fecha y el nombre del recolector de las pruebas. De tal forma se mantiene un registro de a quién debe acudir en caso que las pruebas muestren diferencias desde su punto de partida de la escena del crimen, hasta su recorrido al interior de los diferentes recintos públicos por los que estas deban pasar.

### *2.1.2. Protocolos de Aseguramiento de la Escena del Crimen*

La escena de un crimen, vista como un conjunto de elementos, se considera como un espacio en el cual la víctima, el atacante y su entorno físico, interactuaron entre sí. Es por esto que es de suma importancia que ésta se preserve lo más intacta posible una vez se llegue a dicho lugar. El entorno que se mencionó inicialmente, es el principal recurso preliminar de la investigación criminal. Bajo esta premisa, es necesario poder asegurarlo de principio a fin en el caso tratado.

Al llegar a una escena del crimen hay un factor determinante en la manipulación inicial, la urgencia del caso, que debe ser determinada por un primer respondedor independientemente de la entidad de fuerza pública a la que éste pertenezca. Se considera urgente un acto como la inspección al lugar de los hechos, inspección al cadáver, entrevistas, interrogatorios y situaciones de flagrancia [18]. Si el caso a tratar se clasifica como urgente, se debe reportar inmediatamente a centros de servicios judiciales (CSJ) mediante medios de comunicación al alcance del respectivo primer respondedor encargado. Luego de tener la orden del CSJ para inspeccionar el lugar del crimen, se inicia el proceso, documentando todo sobre los Elementos Materiales Probatorios, evidencia física y en general el estado original de la escena. Adjunto a esto se debe diligenciar la Noticia Criminal, el informe ejecutivo y el formato de reporte de iniciación. Todo debe llegar a manos de un fiscal que deberá tomar el caso y decidir con base en la documentación entregada, cómo se debe seguir el proceso y qué

tipo de personal requiere [18]. En seguida, el mismo fiscal debe determinar un esquema de trabajo para el caso, relacionando su alcance de acuerdo a los recursos con los que cuenta.

De no ser un caso considerado como urgente, se debe diligenciar la Noticia Criminal y enviar al CSJ para ser procesada. En [18] se puede encontrar el formato de la noticia criminal, el informe ejecutivo y el formato de reporte de iniciación.

Luego de determinar la urgencia del caso y de tener la orden de inspección del lugar del crimen aprobada así como los técnicos y especialistas necesarios, se procede a asegurar la escena del crimen; y de considerarse necesario un determinado perímetro o serie de lugares relacionados con ésta. Se debe tener el mayor cuidado posible con el tratamiento del lugar de los hechos ya que la alteración o manipulación incorrecta puede entregar resultados erróneos que desvíen el curso de la investigación. Con este proceso se busca encontrar ya sea evidencia física o elementos materiales probatorios que incriminen un(os) posible(s) autor(res) o sospechoso(s) con el crimen. En caso de encontrar algún elemento físico incriminado, la policía judicial es la única que puede responder a la cadena de custodia sobre dicha evidencia.

Dentro de los informes el lugar de los hechos se puede clasificar según el ambiente en que se encuentre ubicado, por esta razón se generan distintos tipos de escenas del crimen, que son las siguientes: [75]

- Abiertos: Los cuales se caracterizan por no tener límites precisos y, por lo general, pueden consistir en un parque, la vía pública, un potrero, la playa, el campo, etc.
- Cerrados: Se diferencian de los abiertos porque están circunscritos por límites precisos como el interior de una oficina, edificio, un hotel, un supermercado, etc.
- Semi-abiertos o mixtos: Como su nombre lo indica, son aquellos lugares que tienes características propias de los lugares abiertos y a la vez cerrados, como un parque de diversiones, una residencia, un club, etc.

El siguiente proceso es el sugerido por la Policía Judicial colombiana para el tratamiento y análisis de la escena del crimen.

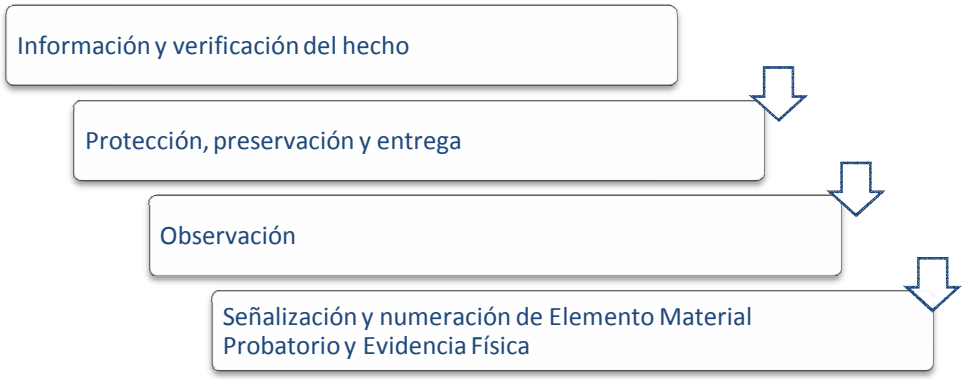


Ilustración 2 Tratamiento y Análisis de la Escena del Crimen

- Información y verificación del hecho: busca relacionar los informes de la Noticia Criminal, informe ejecutivo y el formato de reporte de iniciación con la actual escena del crimen, de tal manera que todo lo redactado en estos reportes se pueda comprobar con lo observado en ese momento.
- Protección, preservación y entrega: se restringe el ingreso al lugar de los hechos al equipo técnico de la policía judicial quien debe iniciar todos los procedimientos de cadena de custodia.
- Observación: en esta etapa se pretende reconstruir el crimen basado en el estado de la escena, encontrando Elementos Materiales Probatorios (EMP) o concretamente Evidencia Física (EF). Teniendo en cuenta que hay evidencia que puede estar parcialmente destruida, se debe determinar sí se debe reconstruir o recuperar posteriormente en un laboratorio, o si se descarta por su maltrato. Teniendo en cuenta el espacio o terreno a analizar, es fundamental crear un plan de observación basándose en un método para recorrer la escena. Los métodos son los siguientes:
  - ✓ Punto a punto.
  - ✓ Por sector o cuadrante.
  - ✓ Círculos concéntricos o espiral.
  - ✓ Por franjas o líneas.
  - ✓ Por cuadrícula o rejilla.

- Señalización y numeración de los EMP y EF: todos los EMP y EF encontrados en la etapa anterior se deben numerar ya sea con un sistema numérico, alfabético o alfanumérico. Independientemente del sistema, el fin es poder identificar cada uno de los hallazgos. Por lo general, el sistema utilizado se relaciona con el método de recorrido utilizado.

Para finalizar todo el análisis, es de suma importancia poder relacionar la EF o EMP con un respectivo documento que muestre qué es, cómo se halló y por qué se debe considerar dentro del caso. Para responder la respuesta del qué es, se puede recurrir a la fotografía o a un video en caso de necesitar una larga secuencia de fotos. Luego se recomienda hacer un diseño topográfico de la escena del crimen, en donde se ilustre claramente cada una de las fuentes de evidencia con su respectiva numeración y señalización para una posible reconstrucción de la escena en un laboratorio en caso que por cualquier circunstancia la escena se altere.

Adicionalmente, en Colombia existe un procedimiento detallado que se debe seguir para asegurar una escena del crimen, está se describe en el "*Manual de procedimientos del sistema de cadena de custodia*" proporcionado por la Fiscalía General de la Nación, donde en primera instancia se define el aseguramiento de la escena como la *"Actividad que se adelanta para garantizar el aseguramiento o protección del lugar de los hechos con ocasión de una posible conducta punible, a fin de evitar la pérdida o alteración de los elementos materia de prueba o evidencia física.*" [73]; lo cual se consigue con la aplicación del siguiente proceso: [73]

1. Realizar una observación preliminar del lugar de los hechos y los EMP o la Evidencia Física, especialmente aquellos que se encuentran a mayor distancia del cuerpo del occiso cuando se trate de inspección a cadáver. El responsable de estos es Policía de Vigilancia y/o Policía Judicial.
2. Determina el área a ser aislada y acordonada, utilizando doble barrera física (cuerdas, cintas, barricadas, policías adicionales, vehículos, voluntarios, entre otros) lo cual permite a los funcionarios adelantar la diligencia ubicándose dentro del perímetro del primer y segundo acordonamiento, dejando el primer acordonamiento para aislar el

lugar de los hechos. El responsable de estos es Policía de Vigilancia y/o Policía Judicial.

3. Realiza el acordonamiento teniendo en cuenta las características del lugar de los hechos. Si el lugar es abierto se toma como referencia el cuerpo de la victima si se trata de una inspección a cadáver y acordona hasta el EMP o EF más alejado de éste. De igual manera procede en otro tipo de conducta, teniéndose en cuenta el área focal más afectada.

   Si el lugar es cerrado, se realiza el acordonamiento desde el punto de acceso al inmueble o inmuebles involucrados en el hecho (puede llegar hasta varias cuadras alrededor del mismo). Es indispensable tener en cuenta las puertas, ventanas y vías probables de escape. El responsable de estos es Policía de Vigilancia y/o Policía Judicial.
4. Reporta a la central de comunicaciones las actividades realizadas. El responsable de estos es Policía de Vigilancia y/o Policía Judicial.
5. Cuando se encuentren personas lesionadas en el lugar de los hechos, se establece comunicación con ellas con el fin de identificarlas y obtener información acerca de lo ocurrido y que sea de interés para la investigación.

   Previo al desplazamiento o movimiento de los lesionados, se procede a marcar la ubicación y posición original de la persona.

   Si se trata de una persona fallecida, se evita su manipulación, la de sus documentos y pertenencias; si en el lugar se encuentran testigos o familiares, se individualizan a través de la información que ellos aporten. El responsable de estos es la Policía de Vigilancia y/o Policía Judicial.
6. Si se encuentran testigos, sospechosos o familiares del occiso o del hecho, se evita que estos se retiren, se procede a separarlos y a aislarlos, impidiendo la comunicación entre ellos.

   Adicionalmente, se toman los datos generales de identificación (nombre, cédula de ciudadanía, parentesco con la víctima, lugar de residencia, entre otros datos). Ésta información se consigna en el formato de actuación del primer respondiente. El responsable es la Policía de Vigilancia y/o Policía Judicial.

7. Si en el lugar de los hechos se encuentra el presunto agresor y es ubicado, se efectúa la requisa de acuerdo al procedimiento establecido, para esta actividad y se separa de los posibles cómplices.

   En caso de que el agresor porte un arma, se incauta teniendo en cuenta lo siguiente:

   - Realizar solo la manipulación estrictamente necesaria, utilizando guantes desechables de látex.
   - Si el arma tiene residuos de fluidos biológicos se coloca preferiblemente en bolsa de papel que no esté pre impreso.
   - El arma embalada, rotulada y con registro de cadena de custodia, se coloca a disposición de la autoridad judicial junto con la información obtenida. (si se trata de policía de vigilancia deja constancia en el formato de actuación del primer respondiente). El responsable de estos es Policía de Vigilancia y/o Policía Judicial.

8. Registra la información obtenida en sus actividades durante la atención al hecho en el formato de actuación del primer respondiente. En caso de observarse que el cuerpo ha sido manipulado o movido del lugar, se deja constancia en el anterior formato.

   Entrega el lugar de los hechos a la autoridad competente o al servidor encargado de la diligencia, aportando el formato de actuación del primer respondiente. El responsable de estos es la Policía de Vigilancia y/o Policía Judicial.

En este mismo documento, se definen una serie de diagramas de flujo que describen de una manera más sencilla, el aseguramiento de la escena del crimen. Dichos diagramas se describen en las siguientes imágenes:

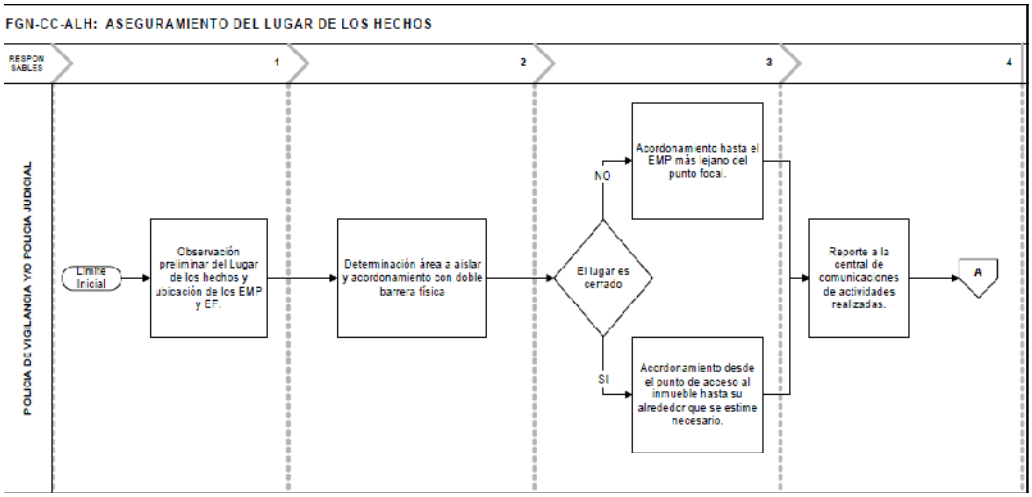


Ilustración 3 Diagrama de Flujo Aseguramiento del Lugar de los Hechos [73]

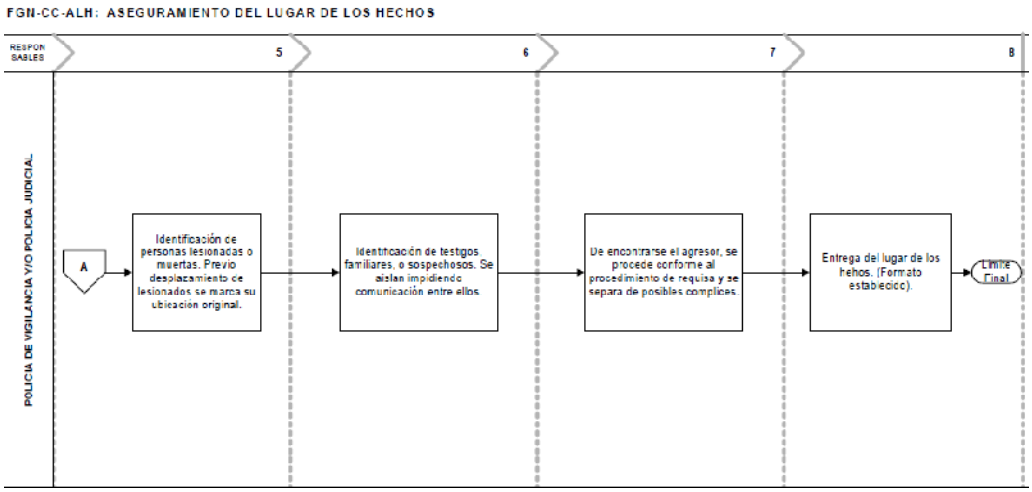


Ilustración 4 Diagrama de Flujo Aseguramiento del Lugar de los Hechos [73]

### *2.1.3. Valoración de EMP*

Los EMP forman parte de la escena del crimen; estos son elementos u objetos (sólidos, líquidos o gases) [75], que según la definición del "*Manual de procedimientos del sistema de cadena de custodia*" se define como: Los elementos físicos que se recaudan por un investigador como consecuencia de un acto delictivo, los cuales pueden servir en la etapa del juicio para demostrar que la teoría del caso que se expone ante el juez es cierta y verificable.

Asimismo, son elementos relacionados con una conducta punible que sirven para determinar la verdad en una actuación penal.

Estos elementos se pueden clasificar de la siguiente manera: [75]

- Según su naturaleza, pueden ser orgánicos e inorgánicos.
- Según su tamaño, pueden ser macroscópicos y microscópicos o elementos traza.
- Si han sido dejados en el lugar de los hechos primarios, pueden ser positivos o negativos.
- Si pueden ser transportados al laboratorio, pueden ser concretos y/o descriptivos.
- Según su capacidad individualizadora, pueden tener características individuales y de clases.
- Según sus características específicas, pueden ser fijos y móviles.

## 2.2. Criminalística Digital – Informática Forense: Resumen de los modelos forenses

### *2.2.1. Informática Forense*

La informática forense es una disciplina que surge como rama de la criminalística, con el fin de proporcionar una respuesta al constante surgimiento de vulnerabilidades en sistemas informáticos, en el aprovechamiento de fallas bien sea humanas, procedimentales o tecnológicas sobre infraestructuras de computación, la cual proporciona un escenario ventajoso y productivo para la generación de tendencias relacionadas acciones mal intencionadas o ilícitas [81].

Esta disciplina se basa fundamentalmente en los principios generales de cualquier investigación forense en criminalística, ellos son [7]:

- Considerar el sistema completo.
- Registrar la información a pesar de las fallas o ataques que se generen.
- Considerar los efectos de los eventos, no sólo las acciones que la causaron.
- Considerar el contexto, para asistir en la interpretación y entendimiento de los eventos.

- Presentar los eventos de manera que pueden ser analizados y entendidos por un analista forense.

Partiendo de dichos principios, la informática forense establece un nuevo conjunto de herramientas, estrategias y acciones en medios informáticos, logrando así recolectar la suficiente evidencia digital que sustente y verifique todas las afirmaciones realizadas sobre el caso bajo estudio [11]. El FBI proporciona una definición más detallada como se menciona en la sección 1.1 del presente documento.

Si se observa la informática forense desde un punto de vista más operativo y técnico, se puede definir como el uso de herramientas software y protocolos para buscar eficientemente los contenidos de almacenamientos magnéticos y otros dispositivos e identificar evidencia relevante en archivos, fragmentos o documentos borrados, que permitan elaborar hipótesis coherentes y válidas relacionadas con el caso de estudio [8].

De acuerdo al segundo objetivo de la informática forense, definido como la persecución y procesamiento judicial de los criminales, es imperativo que la disciplina cuente con un riguroso protocolo de investigación que sustente cualquier afirmación relacionada con el caso de estudio, en esta dirección se plantean inicialmente los siguientes requerimientos para ejecutar una investigación [7]:

- Se deben utilizar medios forenses estériles.
- Mantener la integridad del medio original.
- Cadena de custodia: Etiquetar, controlar y transmitir adecuadamente las copias de datos, impresiones y resultados de la investigación.
- Presentación y sustentación de los resultados.
- Validación y verificación de los procedimientos aplicados.

El tener una lista de requerimientos tan exigente y de alta prioridad, obliga a que la informática forense se valga de un proceso bien definido, donde indique que hacer, en qué momento y quiénes son sus responsables, para que así, se pueda llegar a conclusiones y aseveraciones lo suficientemente argumentativas y comprobables. Por esta razón surgen distintos protocolos y buenas prácticas para la realización de investigaciones forenses, entre

ellas la que propone el IOCE [11] y el Departamento de Justicia de los Estados en su "Guide for First Responders" [47].

Éstas buenas prácticas y protocolos se basan fundamentalmente en la anatomía de una investigación forense, la cual se presenta en la ilustración 5; donde se describe el flujo y proceso general que abarca una investigación.

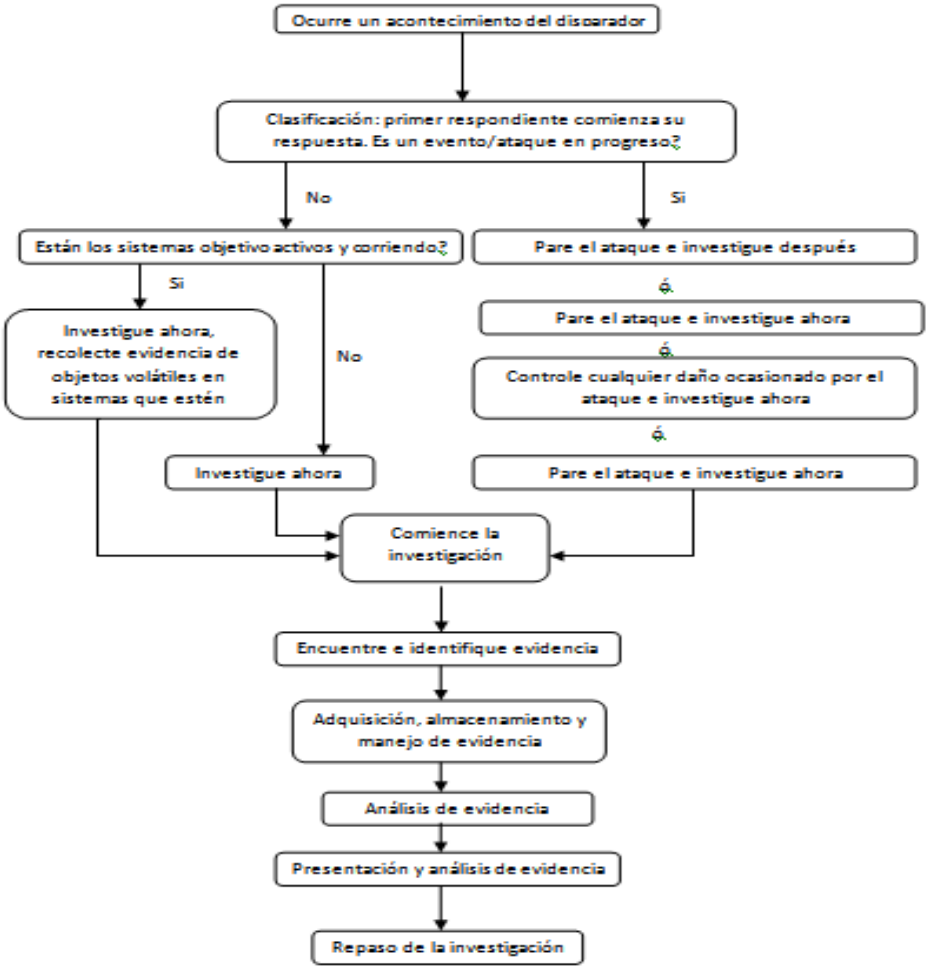


Ilustración 5 Anatomía de una Investigación Forense (traducción) [80]

Como se puede observar, la protagonista en el proceso de una investigación forense es la evidencia digital, ella hace parte de la más importante entrada para el flujo de dicho proceso y la que asegura la sustentación de afirmaciones y conclusiones al momento de presentar

resultados a las entidades judiciales, encargadas de emitir veredictos sobre los casos de estudio.

Por esta razón, se hace necesario que los investigadores de informática forense conozcan a profundidad las características de la evidencia digital, así como cuáles son las distintas formas de generación y los posibles lugares donde se puede encontrar.

### *2.2.2. Resumen de Modelos de Informática Forense*

Como resultado del rigor que se debe tener a la hora de realizar una investigación forense, y la necesidad de un enfoque metodológico claro y bien definido, surgen distintos modelos y metodologías para cumplir con este objetivo. Las cuales proporcionan una amplia diversidad de argumentos y procesos en aras de esquematizar metodológicamente la investigación.

A lo largo de la historia de la informática forense, nacen estándares y buenas prácticas que responden a la necesidad de países y organizaciones de tener herramientas eficientes para realizar investigaciones de cómputo forense, además de proporcionar resultados concluyentes y claros que se acoplen a las exigencias legales vigentes. De manera que se puedan usar, si así se desea, en un proceso legal de enjuiciamiento a los responsables de los posibles ataques.

A continuación se resumen el proceso de algunos estándares y buenas prácticas:

#### *2.2.2.1. RFC3227 (Guidelines for Evidence Collection and Archiving):*

Escrito por Dominique Brezinski y Tom Killalea investigadores del Network Working Group en febrero del 2002, el cual tiene como objetivo ofrecer una guía para la recolección y manejo de la evidencia digital en un incidente de seguridad. Asimismo, busca proveer el manejo adecuado de la evidencia para obtener elementos probatorios contundentes a la hora de efectuar cualquier acción legal contra el intruso.

A continuación se describen los pasos principales que se sugieren en esta guía: [5] y [8]:

1. Directrices para la recolección de evidencia:

- Mantenga adherencia estricta a su política de seguridad organizacional y a su relación formal con el equipo de atención de incidentes así como con las personas responsables del campo jurídico.
- Capture la escena del incidente lo más preciso posible.
- Mantenga notas detalladas. Éstas deben incluir fechas y horas. Si es posible generar un reporte automático, es decir contar con un script, que pueda ser usado para generar un archivo como parte de la evidencia.
- Establezca las diferencias entre el reloj del sistema y la hora de referencia internacional, GMT.
- Esté preparado para testificar (posiblemente años después) detallando las acciones adelantadas y en qué momento. Sus notas detalladas son vitales.
- Minimice los cambios en los datos que ha recolectado. Debe evitar la actualización de horas o fechas en archivos y directorios.
- Remueva posibles formas externas de modificación de la información.
- Primero recolecte la información y luego analice sus hallazgos.
- Aunque usted necesita indicar que sus procesos de atención de incidentes son realizables, debe asegurar su viabilidad y funcionamiento en una crisis.
- En la revisión de cada dispositivo o mecanismo presente en el incidente, se debe seguir un acercamiento metódico para la recolección de evidencia. La rapidez y claridad es crítica para una adecuada y oportuna recolección de evidencia. Es importante efectuar este proceso gradualmente.

2. Recolección de evidencia partiendo desde el siguiente orden de volatilidad:


Ilustración 6 Recolección según orden de Volatilidad

3. Aspectos adicionales para tener en cuenta en la recolección de evidencia:
   - No apague el sistema hasta que la recolección de la evidencia se haya completado.
   - Mucha evidencia se puede perder y el atacante puede haber alterado el proceso de inicio/apagado y las rutinas de inicio de los servicios para destruir la evidencia.
   - No confíe en los programas del sistema. Ejecute programas de recolección de evidencia apropiados, que protejan adecuadamente los medios originales.
   - No ejecute programas que modifiquen las fechas de acceso a todos los archivos del sistema.
   - Cuando remueva dispositivos de acceso externo, note que una simple desconexión o filtro de la red puede disparar la alarma de "switches caídos" que una vez detectados pueden eliminar evidencia en la red.

#### *2.2.2.2. Investigación de la escena de crímenes electrónicos: Guía para primer respondiente (Departamento de Justicia de los Estados Unidos)*

El Departamento de Justicia de los Estados Unidos publicó en el 2001, una guía para el primer nivel de respuesta en escenas de crímenes electrónicos; está dirigida para el uso de entidades gubernamentales y otras organizaciones responsables de protección, recolección, manipulación o preservación de evidencia digital [47].

Esta guía consta de las siguientes etapas:

- **Preparación de Herramientas:** Definir y preparar las herramientas y dispositivos que se ajusten a las necesidades del incidente. Se necesita una herramienta y dispositivo dedicado para cada proceso: documentación, recolección, almacenamiento y transporte.
- ***Aseguramiento y Evaluación de la Escena:*** El primer respondiente debe asegurar la escena para proteger la integridad de toda la evidencia. seguidamente debe analizar e identificar donde se puede encontrar la evidencia potencial, con lo que se genera un plan de búsqueda.
- ***Documentación de la Escena del Crimen:*** Creación de un registro histórico donde se describe el detalle de lo encontrado en la escena del crimen. Este se debe crear y mantener como un documento confidencial.
- ***Recolección de la Evidencia:*** Recolección de evidencia física o digital, siguiendo los parámetros de preservación de evidencia descritos por el departamento de justicia. La recolección de evidencia digital se debe realizar con herramientas y dispositivos certificados.
- ***Cadena de Custodia:*** Garantizar que la evidencia no se alterara, dañará o destruirá, en el transporte, embalaje o almacenamiento.
- ***Análisis Forense:*** Los expertos en informática forense realizan el análisis de la evidencia recolectada.
- ***Presentación de Informes:*** Informe que detalla las conclusiones y resultados del análisis forense.

#### *2.2.2.3. Guía para la integración de técnicas forenses con la respuesta a incidentes (National Institute of Standards and Technology - NIST)*

El Instituto Nacional de Estándares y Tecnología NIST, publica esta guía con el objetivo de ayudar a las organizaciones en la investigación de incidentes de seguridad informática, otorgando orientación básica y practica para los equipos con la responsabilidad de efectuar análisis forenses.

Esta guía está conformada por 4 grandes fases, las cuales se describen brevemente a continuación:

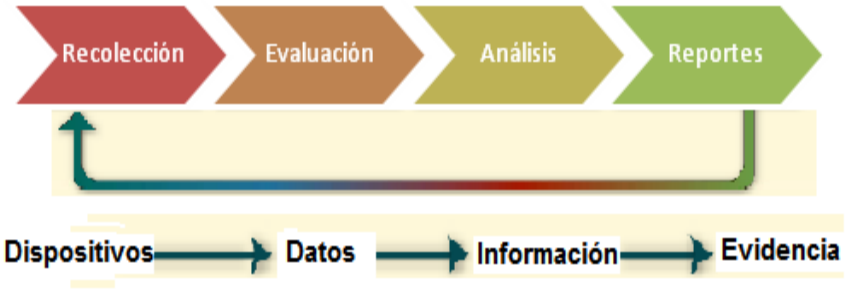


Ilustración 7 Forense NIST (Traducción) [48]

- ***Recolección de Datos***

  El primer paso es identificar las principales fuentes de datos y recolectarlos de la forma adecuada. Para la recolección se deben tener en cuenta los siguientes aspectos:

  - ✓ Identificar fuentes de datos: Buscar en los lugares más comunes de almacenamiento, ejemplo computadores, servidores, portátiles, dispositivos de almacenamiento masivo. Identificar lugares no comunes donde puedan existir datos relevantes.
  - ✓ Recolección de los datos: Es muy importante diseñar y seguir un plan de recolección, tal como: prioridad e importancia según experiencia, volatilidad de los datos, cantidad de esfuerzo requerido. Terminada la recolección se debe realizar la respectiva validación de integridad de los datos obtenidos en este paso.

- ***Evaluación***

  Identificar información relevante de los datos adquiridos en el paso anterior, según escenario del incidente.

- ***Análisis***

Una vez la información relevante se ha extraído, el analista debe estudiar y analizar los datos con la que sacará conclusiones sobre lo ocurrido en el incidente. Este análisis de debe realizar con un enfoque metodológico claro, que permita llegar a conclusiones adecuadas basándose en la evidencia recolectada.

- ***Informes y Reportes***
  Se presentan los resultados y conclusiones del paso de análisis.

## 2.3. Técnicas Anti-Forenses

### *2.3.1. Definición de Técnicas Anti-Forenses*

Las herramientas o técnicas anti–forenses se definen según (Harris, 2006) como "*cualquier intento de comprometer la disponibilidad de la evidencia para un proceso forense."*[27] Del mismo modo, si se profundiza un poco más en éste concepto, y se desarrolla en términos más técnicos se obtiene la siguiente definición: "Cualquier intento exitoso efectuado por un individuo o proceso que impacte de manera negativa la identificación, la disponibilidad, la confiabilidad y la relevancia de la evidencia digital en un proceso forense" [11].

Estas técnicas proporcionan a los atacantes una ventaja inusual sobre los investigadores en cómputo forense, ya que al hacerse efectivas sobre la evidencia digital, pueden comprometer fácilmente la confianza y claridad de la misma, en un proceso.

Así mismo, sugiere a los investigadores observar con un mayor detalle las evidencias digitales encontradas en una escena del crimen, lo que exige replantear los protocolos para investigaciones pasadas y futuras.

### *2.3.2. Clasificación de los Métodos Anti-Forenses*

A medida que se explora y se investiga más sobre las técnicas anti-forenses se han generado varias clasificaciones y se han definido varios métodos. Para efectos de este trabajo se tomará la clasificación planteada por (Harris 2006) a saber [2] :

- Destrucción de la evidencia.

- Ocultar la evidencia.
- Eliminación de las fuentes de la evidencia.
- Falsificación de la evidencia.

La sofisticación y complejidad de cada uno de estos métodos demuestra que los personajes interesados en su creación y ejecución -llamados normalmente intrusos- realizan muchas más cosas y acciones que lo que indican los manuales de los proveedores de software o hardware. [13]

A continuación se establece una aproximación a cada método propuesto por Harris de las herramientas anti-forenses:

- *Destrucción de la evidencia:*

  El principal objetivo de esta técnica es evitar que la evidencia sea encontrada por los investigadores y en caso de que estos la encuentren, disminuir sustancialmente el uso que se le puede dar a dicha evidencia en la investigación formal. Este método no busca que la evidencia sea inaccesible si no que sea irrecuperable. [2]

  Esto implica que se deben destruir, desmantelar o en su defecto modificar todas las pruebas útiles para una investigación [27]. Así como en la vida real cuando ocurre un crimen y el criminal quiere destruir todo rastro o evidencia se vale de una serie de herramientas que le facilitan este objetivo.

  Existen dos niveles de destrucción de la evidencia [2] :

  - ✓ Nivel Físico: A través de campos magnéticos.
  - ✓ Nivel Lógico: Busca reinicializar el medio, cambiar la composición de los datos, sobrescribir los datos o eliminar la referencia a los datos.

  Existe una variedad de herramientas para la destrucción de evidencia de las cuales se pueden valer los intrusos para realizar este método anti-forense. Un ejemplo de herramientas son: Wipe, Shred, PGP Secure Delete, Evidence Eliminator y Sswap [2].

- *Ocultamiento de la Evidencia:*

Este método tiene como principal objetivo, hacer inaccesible la evidencia para el investigador. No busca manipular, destruir o modificar la evidencia sino hacerla lo menos visible para el investigador. [27]

Esta técnica puede llegar a ser muy eficiente de ser bien ejecutada, pero conlleva muchos riesgos para el atacante o intruso, puesto que, al no modificar la evidencia de ser encontrada puede ser válida en una investigación formal y por lo tanto servir para la incriminación e identificación del autor de dicho ataque.

Este método puede valerse de las limitaciones del software forense y del investigador atacando sus puntos ciegos o no usuales de búsqueda de alguna anomalía. [27]

Una de las herramientas utilizadas por los atacantes es la esteganografía, la cual versa sobre técnicas que permiten la ocultación de mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia. [30] En el mercado se pueden encontrar muchos instrumentos fáciles de usar, de bajo costo que pueden ayudar a realizar esta técnica anti-forense, como por ejemplo StegoArchive [62].

- *Eliminación de la fuentes de la evidencia:*
  Este método tiene como principal objetivo neutralizar la fuente de la evidencia, por lo que no es necesario destruir las pruebas puesto que no han llegado a ser creadas. Por ejemplo, en el mundo real cuando un criminal utiliza guantes de goma para utilizar un arma, lo que está haciendo es neutralizando y evitando dejar huellas dactilares en el arma. Así mismo en el mundo digital esta neutralización de las fuentes de la evidencia aplica. [27]

  Una de las acciones que los atacantes pueden llevar a cabo para realizar este método anti-forense, es la desactivación de los log de auditoría del sistema que esté atacando.

- *Falsificación de la evidencia:*
  Esta método busca engañar y crear falsas pruebas para los investigadores forenses , logrando así cubrir a el verdadero autor, incriminando a terceros y por consiguiente desviar la investigación con lo cual sería imposible resolverla de manera correcta. El ejercicio de este método se vale en una edición selectiva de las pruebas creando

evidencias incorrectas y falsas que corrompen y dañan la validez de dichas pruebas en una investigación forense formal, por lo cual no podrán ser tomadas en cuenta como evidencias. [27]

Hoy en día existe una amplia gama de procesos de fácil acceso, con documentación detallada y software que automatiza el ataque, los cuales se valen de la definición u objetivo de alguna técnica Anti – Forense. Algunos de estos métodos se listan en la siguiente tabla.

| **Nombre de Técnica** | **Destrucción** | **Ocultamiento** | **Eliminación de la fuente de evidencia** | **Falsificación** |
|---|---|---|---|---|
| Alteración de los MACE | Borrar o sobrescribir información MACE con datos inservibles | | | Sobrescribir con datos que proveen información engañosa a los investigadores |
| Eliminación/limpieza (wiping) de archivos | Sobrescribir contenidos con datos inservibles | Eliminar archivos (sobrescribir el apuntador al contenido) | | |
| Encapsulación de datos | | Esconder poniendo archivos dentro de otros archivos | | |
| Secuestro o robo de sesión | | | | Se crea evidencia para hacerla parecer como un acto mal intencionado de otra persona diferente de la que lo hizo |

| | | | | |
|---|---|---|---|---|
| Archivos/imágenes bomba | | | | Se crea evidencia con el fin de intentar comprometer el análisis de una imagen |
| Deshabilitar logs | | | Información sobre diferentes actividades no es almacenada | |

Tabla 1 Clasificación de Técnicas Anti-Forenses (Traducción) [27]

## 2.4. Windows XP SP3

Windows XP es el sistema operativo más popular desarrollado por Microsoft, que representa el 49% [77] de los sistemas operativos que operan actualmente. Fue el sucesor de Windows 2000 y Windows Millennium, y posee las fortalezas de sus antecesores, pero con mejoras en estándares de seguridad, interfaces gráficas, manejabilidad, Plug and Play[2], mejor estabilidad y rendimiento, y un sistema de soporte más eficiente, entre otras [71].

Desde la primera versión que saco Microsoft en el 2001, se han publicado 3 paquetes denominados *Service Pack,* que son un compendio de actualizaciones de estabilidad, rendimiento y seguridad. Además frecuentemente se están publicando parches y actualizaciones que mejoran cada día el sistema operativo.

El *Service Pack* más reciente y que se tomará como objeto de estudio en este trabajo, es la tercera edición (SP3), que incluye todas las actualizaciones anteriores, y además viene con un componente fuerte en actualizaciones de seguridad. A continuación se describe las principales mejoras que posee el paquete [79]:

[2] Plug and Play: es una arquitectura de Windows XP que admite la funcionalidad Plug and Play punto a punto para los dispositivos de red. La especificación UPnP se diseñó para simplificar la instalación y administración de dispositivos y de servicios de red. UPnP realiza el descubrimiento y el control de los dispositivos y servicios mediante protocolos sin controladores basados en estándares [65].

| | Funcionalidad | Descripción |
|---|---|---|
| Administración | MMC 3.0 | Marco que unifica y simplifica las tareas de administración y gestión de Windows, proporcionando navegación rápida y sencilla a menús, barras de herramientas y flujos de trabajo. |
| MDAC | MSXML6 | Otorga una mayor confiabilidad, seguridad y conformidad con la versión 1.0 de XML y XML schema. También proporciona compatibilidad con XML 2.0 |
| Conexiones Red | Digital Identity Management Service (DIMS) | Permite que los usuarios que se conecten a cualquier equipo unido a un dominio, accedan a todos los certificados y claves de los servicios que preste este equipo. |
| | Peer Name Resolution Protocol (PNRP) 2.1 | Permite conectar los sistemas XP SP3 que utilizan PNRP con los sistemas Windows Vista que utilizan PNRP. |
| | Remote Desktop Protocol 6.1 | Remote Desktop Protocol (RDP), Permite la comunicación entre un Terminal Server y un Terminal Server Client. Ésta conexión está encapsulada y encriptada con TCP. Mejora la conexión entre maquinas que utilizan XP y Vista. |
| | Wi-Fi Protected Access 2 (WPA2) | Soporte de WPA2, uno de los estándares de seguridad en conexiones inalámbricas del estándar IEEE 802.11i |
| | Network Access Protection (NAP) | Plataforma de aplicación de políticas, con el que puede proteger los activos de red. Permite crear políticas personalizadas para disminuir riesgo a la hora de una conexión con otros dispositivos. Realiza actualizaciones automáticas |
| | CredSSP Security Service Provider | Proveedor de servicios de seguridad (SSPI). Permite generar tiquetes o credenciales para conexión desde un cliente a un servidor. Modifica los registros [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa] y |

| | | |
|---|---|---|
| | | [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ Securi tyProviders] |
| Seguridad | Descripciones de opciones de seguridad | En esta versión las opciones y descripciones de seguridad poseen una mejor interfaz grafica y contiene textos más claros y entendibles para el usuario. |
| | Modulo Microsoft Cryptographic | Soporta algoritmos de hash SHA2. Se añadió el modulo de inscripción rsaenh.dll, el cual está certificado por The Federal Information Processing Standard FIPS 140-2 |
| Instalación | Activación del Productos Windows | Permite realizar la instalación sin un código de confirmación de producto; este se pedirá posteriormente cuando el S.O este en uso. Si este código no es proporcionado en 30 días, el S.O caducara. Esto permite que un usuario interactué y conozca el sistema sin tener que comprarlo. |

Tabla 2 Funcionalidades Windows XP SP3 (Traducción) [79]

## 2.5. Sistemas de Archivos

Un sistema de archivos se puede definir de manera simple como un método de almacenar, manipular, acceder o eliminar uno o varios archivos y la información relacionada con estos. De esta manera, lo que varía entre los diferentes sistemas de archivos es la forma en que cada uno de estos realiza éstas cuatro operaciones. En esta sección se podrá encontrar un breve resumen de los sistemas de archivos que actualmente ese encuentra en el mercado con los diferentes sistemas operativos. Igualmente, se analizará la estructura general de los sistemas de archivos principales.

### *2.5.1. Almacenamiento en Sistemas de Archivos*

Los sistemas de archivos, a modo general, almacenan datos en diferentes sectores del disco duro en un arreglo multidimensional que a su vez están contenidos dentro de un cluster, cuya estructura varía por sistema de archivos. Algunos sistemas de archivos manejan tamaños fijos para cluster, otros como NTFS permiten configurar el tamaño desde 512 hasta 4096 bytes.

Estos cluster pueden contener de 1 a 64 sectores. La responsabilidad del sistema de archivos es mantener una tabla de registros que relacione los archivos o carpetas existentes, con la ubicación física de cada cluster o grupos de ellos para los archivos que no alcancen a almacenarse en uno sólo. La variación se da dependiendo de cómo se almacenen los cluster, ya que hay sistemas de archivos que manejan asignación dinámica y otros estática [56].

### *2.5.2. Nombramiento de Archivos*

La manera en que al usuario final se le muestran los archivos, va asociado a un nombramiento dado por el sistema operativo o por él mismo. Cuando manualmente crea uno. Las tablas de registro de cada sistema de archivos deben relacionar los nombres de cada archivo o carpeta existente en dispositivo de almacenamiento. Ésta relación se da en una tabla de asignación de nombres, en donde cada sistema de archivos maneja estructuras o jerárquicas o planas [43].

### *2.5.3. Metadatos*

Para comenzar a hablar de metadatos primero de deben definir. Los metadatos se consideran datos sobre datos, visto desde otro punto de vista, un objeto que tiene información de sobre otro objeto [74]. Al comprender el concepto, se puede decir que los sistemas de archivos, al igual que almacenan los nombres de los archivos, también dentro de la tabla de asignación de nombres, tienen atributos que manejan metadatos. Los más relevantes son los que manejan las estampillas de tiempo, el tipo de objeto contenido y los tipos de permisos que se tiene, entre otros [3].

### *2.5.4. Manejo de Reubicación de Archivos*

Las características que más varían entre los sistemas de archivos antiguos y los actuales, tienen que ver con la forma en que se maneja la reubicación de archivos. Antiguamente, algunos sistemas de archivos planos no permitían el movimiento de archivos a otros directorios ya que tocaba mover los cluster enteros y eso generaba inestabilidad en la tabla de asignación de nombres. Hoy en día gracias al manejo de sectores, se puede reubicar fácilmente cambiando el apuntador inicial de un cluster a uno nuevo. Otra característica es la del truncamiento de archivos, en donde los cluster no deben éstar necesariamente adyacentes

entre sí, sino que pueden estar en ubicaciones diferentes no necesariamente una al lado de la otra [43].

### *2.5.5. Seguridad en los Sistemas de Archivos*

Con la evolución de los sistemas de archivos y dada la intrusión de los metadatos, se ha cambiado e introducido el concepto de seguridad en los datos que se manejan. Hoy en día, se tienen diferentes métodos de control de acceso y permisos de usuarios sobre los archivos, estos se almacenan en forma de metadatos.

### *2.5.6. Sistema de Archivos NTFS*

#### *2.5.6.1. Historia*

NTFS (New Technology File System). Nació en los noventa gracias a la apertura del mercado de la tecnología. En ese tiempo, los sistemas de Microsoft (MS-DOS y Windows 3.x) funcionaban con el sistema de archivos FAT (*File Allocation Table*), que para la época ya había sido lo suficientemente estudiado y no tenía ningún futuro si se quería avanzar en los sistemas, ya que tenía muchas limitantes que eran irremediables. Para que Microsoft pudiese avanzar en la lucha por la apertura en el mercado, se tenía que crear un nuevo sistema de archivos, que por lo menos estuviera a la par del sistema de archivos que poseía Unix, ya que era mucho más fuerte que el que usaban los sistemas Microsoft. Por esta razón Microsoft decidió Unirse con IBM para desarrollar un nuevo sistema de archivos [50].

Con IBM se desarrolló un nuevo sistema de archivos llamado HPFS (High Performance Filing System), con el cual se esperaba competir con Unix. HPFS fue implementado inicialmente en OS/2 1.2 y contenía gran cantidad de utilidades que no eran imaginables con ninguna versión de FAT, ya que HPFS permitía un mejor acceso a los discos duros y brindaba mayor seguridad para las redes que en ese tiempo estaban apareciendo. "*HPFS mantiene la organización de directorio de FAT, pero agrega la ordenación automática del directorio basada en nombres de archivo. Los nombres de archivo se extienden hasta 254 caracteres de doble byte. HPFS también permite crear un archivo de "datos" y atributos especiales para permitir una mayor flexibilidad en lo que se refiere a admitir otras*

*convenciones de nomenclatura y seguridad. Además, la unidad de asignación cambia de clusteres a sectores físicos (512 bytes), lo que reduce el espacio en disco perdido*" [50].

Además en HPFS se adicionó un archivo de atributo, el cual contenía fecha de creación de modificación y acceso. HPFS tenía la gran virtud de intentar colocar los archivos de manera contigua, para que el acceso fuera mucho más rápido y los tiempos de respuesta del sistema se vieran seriamente reducidos.

Aunque posteriormente Microsoft abandonará la investigación ya que HPFS presentará muchos problemas como la gran sobrecarga que implicaba y la baja en el rendimiento con volúmenes mayores a 400 Mb.

Una vez terminaron las relaciones comerciales con IBM, Microsoft retomo la investigación para el desarrollo de un sistema de archivos, lo suficientemente poderoso y seguro para los nuevos sistemas operativos que se desarrollarían. Con este objetivo en mente, tomó algunas de las pautas que fueron usadas para el desarrollo de HPFS y así nació NTFS, el cual fue implantado inicialmente en los sistemas operativos Windows NT aunque no tuvo mucho auge, ya que en ese tiempo gozaba de gran popularidad. Solo hasta el lanzamiento de Windows 2000, éste cobro relevancia con su versión NTFS 5.0.

#### *2.5.6.2. New Technology File System*

NTFS fue inicialmente implementado en Windows NT arreglando muchas de las limitantes que poseía FAT.

NTFS está desarrollado para dar una solución que incluya desempeño, confiabilidad y compatibilidad a los usuarios de Windows, ya que éste se encuentra diseñado para realizar de manera más efectiva y eficiente, operaciones de lectura, escritura y búsqueda de archivos dentro del sistema, además que provee funcionalidades relativamente más complejas como restauración del sistema de archivos en discos de gran tamaño [34].

La Plataforma estructural de NTFS, es una base de datos que contiene absolutamente toda la información de los "objetos" que se encuentren almacenados bajo el volumen que esté usando NTFS. Ésta base de datos se llama MFT (Master File Table - Tabla de archivos Maestra) y

considera a todos los "Objetos" como Archivos menos al Partion Boot Record (Ver Ilustración 8).

Una de las mayores Ventajas de NTFS, es que es escalable, gracias a que la MFT posee un espacio del 12.5% del espacio total del volumen donde se encuentre operando. Ésta partición es comúnmente conocida como "MFT Reserved Area". De esta manera se evita que la tabla se parta o se relocalice a medida que vaya creciendo, evitando de esta manera la fragmentación que llevaría a una baja en el rendimiento del sistema. [60]

El sistema de archivos como tal, recae sobre una serie de archivos que son los archivos de meta data y que se encarga de los cálculos de asignación de espacios de almacenamiento, Información para la recuperación de archivos y listados de los atributos de los datos almacenados. Estos archivos son invisibles para los ojos de los usuarios.


Ilustración 8 Estructura NTFS [51]

Una vez al volumen se le da formato NTFS y durante la configuración se crea el Master Boot Record o también llamado Partition Boot Record o Partition Boot Sector, que contiene una pequeña parte de código que es llamado Master Boot code y una tabla de particiones del disco, el MBR ejecuta este código dándole control al Boot Sector. La tabla de partition posee información del sistema Incluyendo el Id en el cual se encuentra especificado el sistema de archivos que se maneje. La primera información que se encuentra en el volumen es el "Partition Boot Sector" que se encuentra entre el sector 0 del disco y puede llegar a estar hasta el sector 16. Posteriormente el primer archivo que monta es la MTF para que después con ayuda de la misma este busque los system files y demás archivos para el inicio de la maquina (Ver ilustración 9).

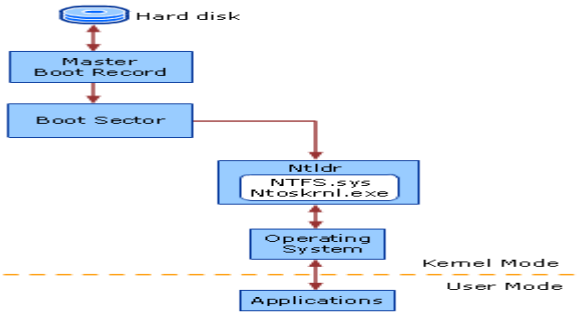


Ilustración 9 Proceso NTFS [42]

| Component | Component Description |
|---|---|
| Hard disk | Contains one or more partitions. |
| Boot sector | Bootable partition that stores information about the layout of the volume and the file system structures, as well as the boot code that loads Ntldr. |
| Master Boot Record | Contains executable code that the system BIOS loads into memory. The code scans the MBR to find the partition table to determine which partition is the active, or bootable, partition. |
| Ntldr.dll | Switches the CPU to protected mode, starts the file system, and then reads the contents of the Boot.ini file. This information determines the startup options and initial boot menu selections. |
| Ntfs.sys | System file driver for NTFS. |
| Ntoskrnl.exe | Extracts information about which system device drivers to load and the load order. |
| Kernel mode | The processing mode that allows code to have direct access to all hardware and memory in the system. |
| User mode | The processing mode in which applications run. |

Ilustración 10 Componentes de una partición NTFS [42]

A continuación se presenta una tabla en la cual se muestra como se encuentra compuesto un volumen que posee NTFS:

| Component | Description |
|---|---|
| NTFS Boot Sector | Contains the BIOS parameter block that stores information about the layout of the volume and the file system structures, as well as the boot code that loads Windows Server 2003. |
| Master File Table | Contains the information necessary to retrieve files from the NTFS partition, such as the attributes of a file. |
| File System Data | Stores data that is not contained within the Master File Table. |
| Master File Table Copy | Includes copies of the records essential for the recovery of the file system if there is a problem with the original copy. |

Ilustración 11 Composición NTFS [42]

Posteriormente se entrará a discutir cada uno de estos componentes.

**Partition Boot Sector**

Cuando se da formato con NTFS el programa se encarga de asignar los primeros 16 sectores del disco para el boot sector y el código del bootstrap.

| Byte Offset | Field Length | Field Name |
|---|---|---|
| 0x00 | 3 bytes | Jump Instruction |
| 0x03 | LONGLONG | OEM ID |
| 0x0B | 25 bytes | BPB |
| 0x24 | 48 bytes | Extended BPB |
| 0x54 | 426 bytes | Bootstrap Code |
| 0x01FE | WORD | End of Sector Marker |

Ilustración 12 NTFS Boot Sector [52]

En la ilustración anterior se pueden ver las instrucciones que se ejecutan en el partition boot sector para comenzar. La carga de BPB (BIOS parameter block) y Extended BPB, estos son bloques que poseen la información propia del volumen y en el Extended BPB se encuentra información de alto nivel como lo es la de la localización de las estructuras de metadata. Estos dos bloques hacen posible que NTLDR pueda encontrar la MFT al iniciar el computador [35]. NTLDR significa NT Loader o el cargador de NT, el cual es el encargado de realizar el arranque (boot) del sistema. Para realizar el arranque en un sistema con sistema operativo basado en NT no es solamente necesario el archivo NTLDR sino que también es necesario el archivo Boot.ini que contiene la información menú, para el arranque y el

Ntdetect.com que es el encargado de identificar el hardware actual del sistema. Una vez leídos estos bloques, se pasará al Botstrap Code o executable boot code, que es el encargado de comenzar a cargar el sistema operativo [35]. Finalmente está acaba su ciclo, con el último bloque que es 0x01FEy representa el final del sector. Una vez terminado el proceso NTLDR ya habrá terminado de cargar la Master File Table.

**MFT (Master File Table)**

La Master File Table, es el lugar donde se ubica toda la información acerca de los archivos y la metadata que se encuentra en el sistema y el directorio del sistema. Las entradas que se hallan en la MFT son de 1 Kbyte y solamente los primeros 42 bytes poseen un propósito definido ya que allí estarán albergados los archivos de metadata [10].

La metadata se ubica en una zona llamada la Metadata Zone y ocupa el 12.5 % del total del Volumen. En esta Zona es imposible albergar información a excepción de que el volumen se encuentre lleno y sea necesario como último recurso. Si el espacio de la MTFzone llegara a llenarse es posible modificar el tamaño de la MTF. [61]

- Configuración 1, es la configuración por defecto y reserve aproximadamente el 12.5% del volumen total
- Configuración 2, reserva aproximadamente el 25% para la master file Table
- Configuración 3, Reserva aproximadamente el 35.7% del tamaño total del Disco para la MTF zone
- Configuración 4, Reserva aproximadamente el 50% del Disco. [61].

Cada Registro dentro de la Master File Table posee un número de Registro Único y cada registro es sucesivo, comenzando desde el 0. La posición de un registro especifico se puede hallar multiplicando el número del registro por el tamaño que se especifique para cada registro y se llegará al byte offset (Posición especifica del registro o address). En las primeras versiones de NTFS, no se encontraba este número de registro y esta información se intuyó por la posición que tuviese el registro dentro de la MTF[61].

Al tener la Master File Table, se ubica la información de todos los archivos del sistema, menos el Boot Sector que es lo único que no es considerado como un archivo. Es de esperarse que la Master File Table Tenga un registro de sí misma, ya que ella también es considerada como un archivo. El registro de la Master file table, es el primero en encontrase dentro de la MTF Posee el registro 0 y está representado de la siguiente forma $Mft. El siguiente registro dentro de la Master File table es una copia de la MTF. Los siguientes Registros hasta el 26 son los archivos de metadata que son los encargados de funciones vitales del sistema, como identificación de espacio libre, direccionamiento, etc. Posteriormente vienen los archivos del sistema Cargados por el Bootstrap y finalmente los archivos del usuario.

Por ende todas las operaciones que se realicen con los archivos, tienen que ver directamente con la Master File Table . Operaciones como el Borrado o creación de archivos poseen como backBone a la MTF.

Dependiendo del archivo, el registro puede ser residente y no residente. Si el archivo es residente, se coloca dentro de la MFT ya que es lo suficientemente pequeño para caber y si es muy grande, lo que se busca es un espacio dentro del volumen para poder ubicarlo y posteriormente lo que se coloca en el registro es la dirección donde quedo.

#### *2.5.6.3. Metadatos en NTFS*

El sistema de archivos NTFS, almacena prácticamente todos los datos, tanto los datos de usuario como la gestión interna de datos, en forma de archivos. Los más importantes son un conjunto de archivos de sistema especiales, que son llamados archivos metadata. El prefijo "meta" generalmente se refiere a algo "trascendente" o "más allá", o simplemente auto-referencia. Por lo tanto, los archivos metadata son archivos que contienen datos acerca de los datos, contienen información interna (datos) sobre la "real" de los datos que están almacenados en el volumen NTFS. [36]

Estos metadatos de los archivos se crean automáticamente por el sistema cuando un volumen NTFS es formateada, y se colocan al principio de la partición. El metadato de mayor importancia es el Master File Table (MFT). [36]

La siguiente tabla muestra los archivos de metadatos detalladamente:

| **Sistema del Archivo** | **Nombre del Archivo** | **MFT Record** |
|---|---|---|
| Master File Table | $Mft | 0 |
| Master File Table 2 | $MftMirr | 1 |
| Log File | $LogFile | 2 |
| Volume | $Volume | 3 |
| Attribute Definitions | $AttrDef | 4 |
| Root File Name Index | $ | 5 |
| Cluster Bitmap | $Bitmap | 6 |
| Boot Sector | $Boot | 7 |
| Bad Cluster File | $BadClus | 8 |
| Security File | $Secure | 9 |
| Upcase Table | $Upcase | 10 |
| NTFS Extension File | $Extend | 11 |
| | | 12-23 |
| | $Extend\$Quota | 24 |
| | $Extend\$ObjId | 25 |
| | $Extend\$Reparse | 26 |

Tabla 3 MFT en Windows XP Profesional Versión 2002 SP3 [36], [34], [68].

Una información detallada de cada uno de los atributos se encuentra en [51] y [42].

#### *2.5.6.4. Atributos de los Sistemas de Archivos NTFS*

Como se ha visto todo en NTFS es un archivo y los archivos tienen una colección de atributos. El significado de los atributos depende de cómo el software lo interprete. Por ejemplo una carpeta es almacenada de la misma manera que un archivo pero el uso de los atributos es de diferente manera. [37]

Todos los atributos de los archivos son almacenados en la MFT o en otra localización dependiendo del tamaño del atributo. Las dos diferentes maneras de almacenar un atributo son:

- Atributos Residentes: Son atributos que requieren poco espacio para ser almacenado directamente en la MFT. Los atributos más comunes y simples como el nombre del archivo, su creación, modificación y fecha/hora de accesos están almacenadas en la MFT. [69]
- Atributos No-Residentes: Si un atributo requiere más espacio que el disponible en el registro de la MFT, el atributo es almacenado en otra localización y se coloca un puntero en la MFT que le indica la localización de ese atributo. [69]

Los "system defined attributes" (atributos definidos por el sistema) o los atributos de la MFT con su respectivo identificador son los siguientes:

| **Atributo** | **Identificador** |
|---|---|
| Standard_Information | 10 00 00 00 |
| Attribute_List | 20 00 00 00 |
| File_Name | 30 00 00 00 |
| Object_ID | 40 00 00 00 |
| Security_Descriptor | 50 00 00 00 |
| Volume_Name | 60 00 00 00 |
| Volume_Information | 70 00 00 00 |
| Data | 80 00 00 00 |
| Index_Root | 90 00 00 00 |
| Index_Allocation | A0 00 00 00 |
| Bitmap | B0 00 00 00 |
| Reparse_Point | C0 00 00 00 |
| EA_Information | D0 00 00 00 |
| EA | E0 00 00 00 |
| Logged_Utility_Stream | 00 00 00 00 |

Tabla 4 Identificadores de Atributos de la MFT [61]

- Bitmap

Contiene el mapa de bits de los clusters que son usados por Bitmap.

- Data

  Contiene los datos del archivo. Todos los datos del archivo se almacenan en solo un atributo.

- Extended Attribute (EA) and Extended Attribute

  Son atributos especiales que se implementaron para la compatibilidad con OS/2.

- File Name

  Este atributo almacena el nombre asociado al archivo o al directorio. Un archivo o directorio puede tener varios atributos de nombres de archivo para utilizar nombres regulares como por ejemplo en MS-DOS se usan los nombres más cortos.

- Index Root Attribute

  Este atributo contiene el índice actual de los archivos contenidos en un directorio. Si el directorio es pequeño, el índice completo se coloca en la MFT pero si el índice es muy largo, alguna información se coloca en MFT y el resto se guarda con atributos de índices externos.

- Index Allocation Attribute

  Si el índice de un directorio es muy largo para caber en el "index root attribute", el registro de la MFT del directorio contendrá un "Index Allocation Attribute" que contiene un puntero al "index buffer entries" que contienen el resto de los índices del directorio.

- Security Descriptor(SD)

  Contiene información de seguridad que controla el acceso al archivo o al directorio. Access Control Lists (ACLs) y datos relacionados se almacenan en este atributo.

- Standard Information (SI)

  Contiene información fundamental como fechas y horas de creación, modificación y acceso. También si el archivo es de solo lectura, escondido igual que en FAT.

- Volume Name, Volume Information, and Volume Version

Estos tres atributos, almacenan el nombre de la llave, la versión y otra información relacionada con el volumen NTFS. Estos atributos son usados por el metadato $Volume.

## 2.6. Técnicas Anti-Forenses en Windows

### *2.6.1. Ocultamiento*

Windows XP posee un sistema de archivos NTFS, en el cual cada objeto que se encuentra almacenado en el disco duro es visto como un archivo que contiene una serie de atributos, los cuales pueden ser obligatorios dependiendo del tipo de archivo [29].

Desafortunadamente, NTFS permite que cada archivo contenga más de un atributo que no sea necesario o que este sin uso, lo que abre una brecha para ocultar información sin afectar el correcto funcionamiento del sistema.

Una de las formas más efectivas para ocultar información, es utilizar el atributo de $DATA, puesto que este atributo es el único que se encuentra sin un formato implícito, lo que permite una mayor manipulación en comparación a los demás atributos. De manera que se puede almacenar cualquier tipo de dato y con cualquier tamaño sin llegar a generar sospecha alguna. Por estas razones este atributo ofrece el ambiente ideal para ocultar información sin generar traumatismos o sospechas para los mecanismos de control del sistema de archivos [29].

Ocultar información en este atributo se conoce como métodos de ocultamiento basados en archivos de Metadata. Sin embargo, existen más formas de ocultar información utilizando este método, como lo es el utilizar el archivo $BadClus, que es donde se almacenan todos los clusters marcados como dañados (Bad). Así que todos los clusters que se encuentren en este archivo pueden ser utilizados para ocultar cualquier tipo de información, además se cuenta con un tamaño que es igual a la capacidad con la que cuenta el sistema de archivos [29].

Otra de las formas que utiliza el método de los Metadatos, es ocultar información en el archivo $Boot, específicamente en donde se encuentra Boot Code, el cual es el que le indica al sistema de archivos donde encontrar los archivos necesarios para el arranque del sistema

operativo. La desventaja que tiene esta técnica es el tamaño con el que se cuenta, ya que se ve limitado por el número de la no-cero bytes en el archivo $ Boot.

Aparte de los sitios ya mencionado NTFS provee más lugares para ocultar información, los cuales se pueden explotar con distintos métodos, como utilizar los Alternate Data Streams (ADSs). Los ADSs corresponden a una funcionalidad creada para proveer compatibilidad entre los servidores Windows NT y los clientes Macintosh que usaban Hierarchical File System (HFS). En la MFT (Master File Table) de NTFS existe más un atributo $DATA, y se conoce a estos atributos adicionales como los ADS. Es posible ocultar información en este lugar puesto la mayoría de las utilidades del sistema solo examinan el primer atributo $DATA [29].

Asimismo, también es posible ocultar información en espacio Slack, que se refiere a todos los espacios que no pueden ser utilizados por el Sistema de Archivos por las directivas de almacenamiento, como por ejemplo el espacio fijo que es asignado a un cluster que proporciona un espacio Slack debido a que no siempre la información almacenada en este posee el mismo tamaño.

Existen distintos tipos de espacios Slack en NTFS que pueden ser utilizados para ocultar información, tales como [29]:

- Volumen Slack que corresponde al espacio libre entre el final del sistema de archivos y el final de la partición donde está alojado el sistema de archivos.
- File System Slack que corresponde al espacio sin utilizar al final del sistema de archivos que no ha sido asignado a ningún cluster. Esto puede suceder debido a que el tamaño designado para la partición no sea un múltiplo del tamaño fijo definido para un cluster.
- File Slack es el espacio sin uso que se encuentra entre el final de un archivo y el final del último Cluster asignado. Existen dos tipos de File Slack, que son:
    - ✓ Ram Slack: Corresponde al espacio que inicia en el final del archivo y termina en el último sector utilizado parcialmente del último cluster asignado.

- ✓ Drive Slack: Es el espacio que va desde el inicio del próximo sector que se encuentra en el último Cluster asignado.

### *2.6.2. Eliminación de la fuente de la evidencia*

Windows posee una herramienta llamada Windows Event Log que administra los eventos que ocurren en el sistema y los registra en una serie de logs para su posterior análisis. Esta herramienta proporciona logs de las aplicaciones instaladas en la máquina, losg de procesos propios y que usan funciones y recursos del sistema, logs y alertas de posibles incidentes de seguridad y logs acerca de los productos de office.

Estos logs son de bastante utilidad a la hora de diagnosticar errores en el sistema operativo, con los que se pueden trazar los distintos aspectos que pudieron causar los problemas. Asimismo, son un insumo esencial en cualquier investigación forense, ya que estos logs proporcionan evidencia valiosa e importante.

Los atacantes pueden deshabilitar el servicio de Windows Event Log, para que no registre ninguna acción, por lo que no se genera evidencia en logs que los pudiere incriminar. Ésta operación es bastante sencilla si se tiene un control total de la máquina víctima, ya que solo es dirigirse al Administrador de Herramientas de Windows, seleccionar servicios y buscar el servicio Event Log y detenerlo [66].

Asimismo, existen en el mercado, distintas herramientas que manipulan este servicio, como el Meterpreter de Metasploit [39], que limpia automáticamente todos los logs generados por el servicio Event Log. Esto lo hace utilizando una serie de funciones que posee la librería de este servicio (disponible en Microsoft Development Network) [44].

### *2.6.3. Destrucción de la Evidencia*

Como se explicó en la sección 2.3.2., la destrucción de los datos en Windows al igual que en cualquier sistema operativo, busca hacer la información irrecuperable. Ésta destrucción se materializa mediante algoritmos de borrado seguro los cuales varían acorde a:

- La cantidad de pasadas que se haga sobre el sector del disco.
- La forma en que se sobrescribe.

En el Anexo 5 (Métodos y Herramientas de Borrado Seguro, Tabla 1) se muestra los algoritmos más populares para implementar aplicaciones de borrado seguro o destrucción de datos. Ahí se clasifica cada uno de los métodos que existen para destruir información sobre un dispositivo de almacenamiento masivo con un sistema de archivos NTFS.

Como se puede observar en la tabla 1 del anexo 5, a medida que el grado del método aumenta, aumenta el número de sobrescrituras. Comenzando con un algoritmo que de modo rápido sobrescribe sólo una vez con ceros, hasta llegar a la unión entre el método de Gutmann y el del Departamento de Defensa de los Estados Unidos que realiza el proceso hasta 35 veces con números pseudoaleatorios. Es importante recalcar que los métodos de grado 12, 13 y 14, son exclusivos de agencias gubernamentales y de investigación a nivel internacional, dado que la capacidad de procesamiento debe ser alta ya que los tiempos para ejecutar estos métodos son bastante altos y aumentan dependiendo de la capacidad del dispositivo analizado.

Existen diferentes herramientas en el mercado de software que implementan los métodos de borrado seguro, tanto de licencias comerciales como de licencias públicas, la variación entre ellas depende del grado del método y todo lo que esto atañe.

Al borrar o eliminar un archivo se desencadena una serie de procedimientos dentro del sistema de archivos para realizar la acción. Este procedimiento difiere en algunos pasos según el sistema de archivos y la estructura que este tenga.

En una forma general el proceso de borrado de un archivo en el sistema de archivos NTFS necesita realizar tres cambios [72]:

1. Modificar un byte en el offset (16H) que se encuentra en el encabezado de la MFT (Master File Table), el cual otorga información sobre el archivo a la que hace referencia el registro de la MFT. Este byte pude tener asignado los siguientes valores: 0 significa que el archivo está borrado, 1 significa el archivo está en uso, 2 significa que el registro hace referencia a un directorio de archivos y 3 significa que el directorio está borrado.
2. Identificar el directorio padre en el atributo $INDEX_ROOT de la MFT el cual corresponde al nodo raíz del árbol B+ de índices que posee NTFS [58].

3. Posteriormente utilizando el índice que otorga el root, analizar el $INDEX_ALLOCATION el cual tiene almacenados todos los sub-nodos del árbol B+ de índices [58] para así poder ubicar el $BITMAP y cambiar a cero o uno (dependiendo del método de borrado seguro) los bits correspondientes al archivo que se requiere borrar.

Finalizando el proceso anterior el archivo quedaría borrado, o invisible para el sistema de archivos, pero esto no es del todo cierto ya que los datos a los que apuntaban los índices de la MFT siguen en su lugar, así que es necesario efectuar adicionalmente al proceso ya descrito aplicar técnicas de borrado seguro como lo es el método de Guttman, NAVSO P5239-26, TSSIT OPS-II, DoD, entre otros, los cuales se explicaron anteriormente (Ver Anexo 5).

**Herramientas que realizan destrucción de información y datos.**

En el Anexo 5 Tabla 2 se puede encontrar un listado detallado de herramientas que realizan borrado seguro de discos duros con formato NTFS.

### *2.6.4. Falsificación de la Fuente de Evidencia*

Al falsificar la evidencia, el atacante está generando evidencia que no existe o modificando la existente para que no sea contemplada como tal, o para que, tenga datos falsos los cuales lleven la investigación por otro rumbo. Ésta técnica busca que al aplicarse se desvíe un rastro de la utilización de un sniffer[3], un backdoor[4] o un rootkit[5], entre otros. Las técnicas más conocidas de falsificación de evidencia son las de alteración de los atributos MACE sobre un archivo, registro o carpeta, la del robo de sesión para implicar un usuario diferente al atacante o la de imágenes o archivos bomba el cual busca crear evidencia que altere el análisis de una imagen forense.

[3] Sniffer: Software que está en capacidad de capturar el tráfico de una red.
[4] Backdoor: Es una secuencia de líneas de código dentro de una aplicación informática que mediante malas prácticas de programación implementadas con conocimiento de causa, permiten mantener un vínculo con una máquina víctima de manera permanente o por un determinado periodo de tiempo.
[5] Rootkit: Es una herramienta que permite esconder archivos o procesos que le permiten a un intruso tener el acceso a una máquina. Pueden borrar registros de sus actividades con el fin de evitar ser rastreados [64].

Comenzado por el método de modificación de los atributos MACE, se debe retomar la estructura de la MFT del sistema de archivos NTFS. Es acá en donde se aplican estos cambios a los atributos que cada archivo, carpeta o registro que se encuentre en el disco duro. Para entender de dichas características de los registros del sistema de archivos ya mencionado, se debe entender que estos atributos básicamente son registros de tiempo o time-stamps, que almacenan la fecha de creación, modificación, accedido y modificación de una entrada, MACE. La primera sigla, M, se refiera a la fecha y hora del último cambio que se hizo sobre el atributo Datos de la *Master File Table* de NTFS, lo que normalmente se conoce como "el archivo" [21], la segunda, A, se refiera a la última vez que el archivo se vio envuelto en una actividad, la tercera, C , hace referencia a la fecha y hora en que fue creado, y el último, *entry modified* se refiere al tiempo en que fue modificado por última vez cualquier atributo del archivo dentro de la MFT, como su nombre, metadatos, datos, etc. Al modificar estos atributos se consigue evitar que un analista forense obtenga una línea de tiempo de sucesos en un sistema, dificultando la correlación de eventos y empobreciendo la evidencia digital. Todo lo anterior perturba la etapa de análisis de datos dentro del proceso digital forense.

Como se observa en la tabla 4, de tipos de atributos de los archivos o en general cualquier registro del sistema de archivos (Ver Tabla 4), hay dos tipos de atributo que concretamente tratan los registros de tiempo, los SIA y los FN. La diferencia entre los registros de tiempo del SIA y los de FN es que mientras en SIA la información MACE se modifica cada vez que se lleva a cabo alguna acción sobre un archivo como accederlo o modificarlo, en FN la información solamente se modifica cuando se crea o se mueve al archivo de una ruta a otra [38]. Por lo tanto las fechas y horas MACE registradas en el atributo FN deben ser más antiguas que las registradas en el atributo SIA.

El Secuestro o robo de sesión, se puede definir como un ataque que realiza la explotación de una sesión entre dos o más dispositivos que se comunican mediante una red de comunicaciones sin permiso de ninguna de las partes [22]. El fin principal de un robo de sesión, es interceptar datos para posteriormente poder iniciar remotamente la sesión secuestrada. Protocolos como FTP, Telnet y rlogin que funcionan por naturaleza con sesiones que requieren mantener conexiones activas por largos periodos de tiempo y son fácilmente

auditables por un analizador de tráfico de red [32]. Dichos protocolos le permiten al atacante, omitir la autenticación frente a los servidores que reciben las peticiones, lo que les genera aún más ventajas sobre la máquina víctima. Claro está que las vulnerabilidades de autenticación y registro van ligadas a las tecnologías que envuelven al software y hardware que se tenga.

Identificando cuáles son los protocolos de comunicación que se utilizan durante un robo de sesión y que todos estos necesitan basarse en una comunicación inicial, dada por el protocolo TCP/IP, se toma como punto de partida para una investigación todo el tráfico sospechoso que se tenga con estos protocolos. Igualmente es de vital importancia analizar los logs de eventos de Windows y revisar si se han creado nuevos usuarios y desde qué IP's.

Para el análisis de tráfico se debe tomar como base el three-way-handshake el cual es la base de cualquier comunicación entre computadores. Teniendo en cuenta que los pasos del método son:

1. SYN o solicitud de sincronización con un número de secuencia aleatorio (por lo general).
2. SYN/ACK en donde el servidor recibe la petición del cliente y le avisa al cliente que lo recibió con el mismo número de secuencia más una unidad.
3. ACK en donde el cliente le muestra al servidor que quiere establecer una conexión aumentando en uno el número recibido en el paso anterior con la cual se deja establecida una conexión entre las máquinas.

Luego de realizar este proceso, se establece una conexión mediante Telnet, FTP o rlogin, pero antes de llevarla a cabo y durante el proceso del three-way-handshake se tiene que analizar si hay un cambio de MAC o IP. Para esto es necesario estar monitoreando la red con un sniffer o un sistema de detección de intrusos (IDS). El siguiente pantallazo muestra cómo un sniffer detecta el cambio de una MAC a una IP.

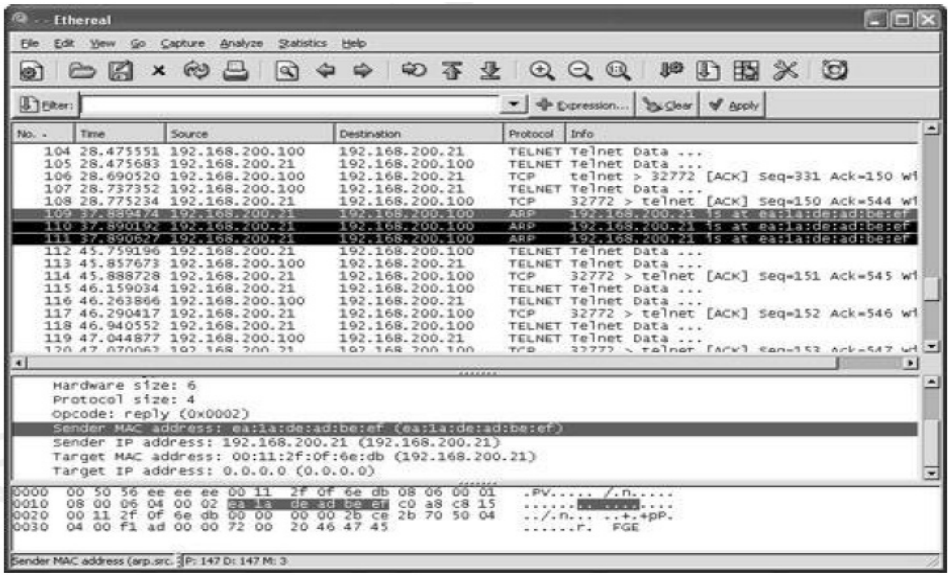


Ilustración 13 Cambio de MAC a una IP [32]

Otra actividad sospechosa a analizar es el secuestro o robo del tráfico. Esto es un proceso relativamente más fácil de detectar, ya que si se analiza el tráfico de los paquetes que se transportan y se encuentra que en algún momento el emisor y receptor cambia su MAC o IP hay una alta probabilidad de que el tráfico esté siendo tomado por una máquina diferente a las que entablaron la comunicación [32].

Finalmente, una actividad que hoy en día no es muy común, es la de inundación de SYN, que consiste en realizar múltiples peticiones de SYN hacia un servidor para que cuando este último responda con el SYN-ACK el cliente o atacante en este caso, nunca le termine el three-way-handshake de tal manera que el servidor se quede esperando el ACK para los diferentes SYN-ACK que se acaba de enviar [23].

## 2.7. Modelo de Detección y Rastreo de Técnicas Anti-Forenses (MoDeRaTA)

Este modelo busca o propone la clasificación e identificación de las técnicas anti-forenses en términos de esfuerzo o sofisticación requeridos por el atacante para ejecutar cualquier técnica, en la determinación de elementos susceptibles a estos ataques y en la identificación de dichas técnicas. [12]

El modelo se describe en la ilustación 14, contiene los niveles de detección y rastreo, niveles de análisis y técnicas utilizadas; donde cada categorización en los distintos niveles tiene las siguientes consideraciones:

- *Niveles de análisis:* Definen los elementos susceptibles donde se pueden materializar las técnicas anti-forenses tales como memoria, proceso, sistema de archivos, aplicación y gestión de la (in)seguridad. [12]
- *Nivel de detección y rastreo:* Establece los rangos y grados en los cuales es posible detectar y rastrear la materialización de técnicas anti-forenses e incluye el nivel de esfuerzo (sofisticación) requerido por el atacante para materializar la técnica anti-forense. [12]
- *Técnicas anti-forenses:* Indica las distintas técnicas (destruir, mimetizar, manipular y deshabilitar la cuales fueron definidas al inicio del documento) que pueden materializarse en los distintos niveles de análisis. [12]


Ilustración 14 MoDeRaTA [12]

Las técnicas anti forenses aplicadas a Windows XP que se detallan en la sección anterior, pueden ser clasificadas en éste modelo. Dicha acción, ayuda a los investigadores de un incidente (que pueda estar basado en técnicas anti-forenses), a obtener una visión general de lo que se debe seguir, en el proceso de esclarecimiento de los hechos. Este modelo otorga dos puntos de vista importantes:

1. El nivel de detección y rastreo de la técnica según el lugar de clasificación; el cual permite a los investigadores generar planes de identificación, búsqueda de

evidencia; selección del tipo de tecnología necesaria en las herramientas, entre otras. (II) El nivel de sofisticación necesaria para la aplicación de la técnica anti forense, que indica el grado de experiencia y conocimientos requeridos por parte de las personas que integren el grupo de investigación.

2. Para efectos de esta investigación sólo se tendrán en cuenta los métodos anti forenses que se clasifiquen en el sistema de archivos del modelo MoDeRaTA. En secciones posteriores, se evaluará y analizará la aplicación de varios de estos métodos orientados a sistemas de archivos NTFS y se realizaran pruebas para comprobar si la información que arroja el modelo concuerda con datos de un incidente de seguridad en un escenario de prueba.

# 3. PROCESO

## 3.1. Guía metodológica para identificar y validar la aplicación de técnicas anti-forenses en equipos con sistema operativo Windows XP SP3

A continuación se describirá la guía metodológica para identificar y validar la aplicación de técnicas anti-forenses en equipos con sistema operativo Windows XP SP3, la cual surge como resultado de la investigación efectuada en este trabajo de grado.

A grandes rasgos, esta guía se divide esencialmente en cuatro etapas que son: Preliminar, Recolección y Clasificación de Información, Análisis de la Evidencia y la Final. Cada una de las etapas se compone de una serie de pasos que abarcan los principales protocolos de análisis forense y adicionalmente, procesos enfocados a la identificación de técnicas anti–forenses en equipos con las características anteriormente mencionadas. En la siguiente ilustración se resume la guía en sus diferentes etapas. Adicionalmente, se muestran los aportes que entregan con ésta y los entregables por cada etapa.

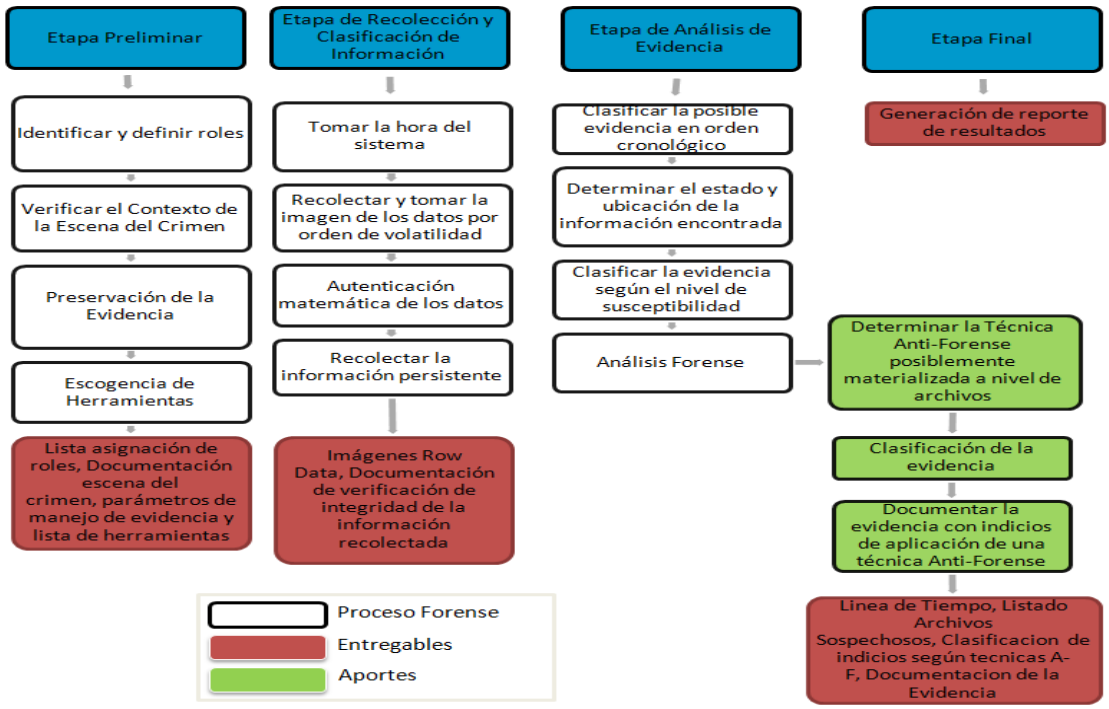


Ilustración 15 Resumen de la guía

**ETAPA PRELIMINAR**

Esta fase tiene como principal objetivo la preparación de los aspectos iníciales en una investigación forense y en la aplicación de la guía, tales como: la definición de roles en el trascurso de la investigación, verificación del contexto de la escena del crimen, preservación de la evidencia y se cierra con la escogencia de las herramientas indicadas para hacer el análisis forense. Así mismo, se entregará un listado de los roles asignados para toda la investigación, un listado de los dispositivos incautados junto con respectiva documentación y finalmente un resumen del por qué se escogió (eron) la(s) herramienta(s) forense(s) tomando como base la tabla comparativa de éstas (Ver Tabla 7).

Estos pasos se toman como referencia para un análisis forense confiable, por tanto se deben contar con los cuidados necesarios que aseguren aspectos claves del proceso de análisis y de la investigación forense.

### *3.1.1. Identificar y definir roles (Paso 1)*

Los diferentes roles que se deben tomar y asignar son vitales para el desarrollo de cualquier tipo de investigación de informática forense. El buen desarrollo de una investigación radica, en buena parte, en la comunicación establecida entre estos roles y el cumplimiento de sus respectivas funciones. A continuación se listan los respectivos roles que Cano propone [14]:

- Líder del caso: es el gestor de caso. Dirige y asigna las actividades del resto de los operarios de la investigación. Debe estar supervisando constantemente que la planeación del caso sea cumplida de la manera en que se estipuló inicialmente, esto incluye que una serie de metas u objetivos planteados, que el contexto de la investigación sea el indicado y que el desarrollo del caso transcurra de la manera prevista. Es designado por la empresa contratada para la investigación o por un ente de justicia y a su vez, designa el resto de los roles.

- Líder de la investigación: es el encargado de establecer los nexos entre los hechos y sus actores. Debe seguir el principio de intercambio de Edmund Locard[6] para determinar los vínculos entre escena del crimen, atacante y víctima, con el único fin de reconstruir el crimen lo más semejante a lo que fue y así poder obtener conclusiones necesarias para resolver el caso.

- Propietario del sistema o negocio: también se le puede llamar víctima. Es quien ha sufrido robo, manipulación o destrucción de información y quien lo denuncia ante autoridades competentes. Inicialmente es la principal fuente de información acerca del caso y los hechos que lo rodean.

- Asesor legal: es el abogado encargado de orientar al líder del caso en sus derechos y obligaciones legales concernientes. Así mismo, debe mantener informado al líder de las consideraciones que se tienen al desarrollar la investigación. Es quien debe conocer la ley, el contexto penal y los aspectos legales que involucra la recolección y presentación de evidencia digital. Tienen el

[6] Principio que propone que en un crimen siempre que hay un contacto entre cualquiera de las partes involucradas (escena del crimen, víctima y atacante), estas se llevan algo la una de la otra [57].

deber de asesorar al líder como testigos expertos ante la audiencia pública, en caso de ser necesario.

- Auditor o especialista en seguridad de la información: es quien debe conocer la topología de la red a tratar y cómo interactúa con los componentes de seguridad de manera interna y externa en la organización [46]. Debe tener conocimiento acerca de las políticas de seguridad de la empresa y la forma de implementación del modelo de seguridad definido por y para los altos mandos administrativos de la organización. Internamente, debe ser quien interactúa con los datos e información recolectada en el caso.

- Administrador del sistema: es la persona que se encarga de gestionar el sistema implantado en la organización, es por esto que debe conocer todas las particularidades de éste. Así, sus responsabilidades se basan en proveer toda la información necesaria a los especialistas en informática forense para tratar de recrear la escena del crimen y el ataque, teniendo en cuenta el funcionamiento de su sistema, para finalmente tratar de encontrar cualquier huella digital dejada por el atacante.

- Especialista en informática forense: es el encargado de dirigir y guiar la investigación en la escena del crimen digital. Líder en la criminalística digital de campo para la investigación; es el encargado de observar, fijar, proteger y conservar el lugar de los hechos, recolecta los hallazgos relacionados con los hechos ocurridos para posteriormente ser analizados en un laboratorio [19]. Con la ayuda del analista de informática forense, debe tratar de establecer el mayor número de vínculos entre hechos y hallazgos en la escena.

- Analista en informática forense: es quien dirige la criminalística digital de laboratorio. Estudia los hallazgos de la escena del crimen, los analiza y los incluye o descarta como evidencia para el caso [19] mediante métodos y técnicas propias de informática forense. Relaciona la evidencia entre sí. Debe valerse de herramientas de software y hardware para sus labores, conociendo su debido funcionamiento. Para el proceso de análisis de evidencia, es necesario que este a

la vanguardia de los ataques y las técnicas utilizadas por los intrusos [14]. Así mismo, debe tener un previo conocimiento de técnicas anti-forenses, los niveles físicos en donde se pueden aplicar, el grado de sofisticación y los posibles rastros que cada una pueda dejar.

### *3.1.2. Verificar que el contexto de la escena del crimen digital presente las características adecuadas (Paso 2)*

En primera instancia, es importante clasificar los elementos que no se contemplan dentro de la investigación en el contexto de este trabajo. Es por esto que para delimitar el alcance, se detalla el listado de equipos no será el centro de la investigación.

- PDAs así tenga cualquier versión de Windows como sistema operativo.
- Celulares de cualquier tecnología y con cualquier sistema operativo.
- Computadores (portátiles o de escritorio) con sistema operativo MAC OS, MAC OSX o cualquier otro sistema operativo de Apple Inc.o Macintosh, cualquier distribución con licencia GPL (GNU Public License), Solaris y derivados, DOS o sistemas operativos basados en UNIX.
- Computadores (portátiles o de escritorio) con discos duros que manejen sistemas de archivos ZFS, ext1-3, HFS, FAT-32, MFS, XFS, QFS o PCFS.

Sin embargo, en caso tal de encontrarse algún vínculo con máquinas con las características anteriormente mencionadas, es necesario documentar su existencia para ser investigados con los protocolos, herramientas y técnicas adecuadas, y así poder relacionarlas con la investigación, sin ser el foco de ésta. Cabe resaltar que es necesario recolectar cualquier dispositivo extraíble de almacenamiento masivo, con el fin de complementar la investigación.

Los equipos que se van a incautar son máquinas con sistema operativo Windows XP SP3 instalado en un disco duro con sistema de archivos NTFS.

A continuación, de ser posible, se debe vincular el o los computadores encontrados, al dueño(s) o usuario(s) para poder preguntarle acerca de los hechos ocurridos y/o datos de registro necesarios para acceder al equipo o a funciones de éste. Es importante documentar la entrevista con el posible sospechoso tomando como información principal el modo de uso de la máquina, la frecuencia de uso, los usuarios del equipo, red a la que pertenece (en caso de hacerlo), software usado, páginas en internet que normalmente se consultan y su frecuencia de acceso, modo de conectarse a internet, proveedor de internet, cuentas de correo electrónico y de mensajería instantánea, información de acceso a redes sociales en internet, si se observaron comportamientos inusuales con el computador últimamente y cualquier otra información relevante [47].

Finalmente, se debe documentar el estado del computador encontrado teniendo en cuenta si se encuentra encendido o no, qué dispositivos tiene conectados a él y si está o no conectado a internet o a una intranet.

### *3.1.3. Preservación de la evidencia (Paso 3)*

Este paso busca principalmente asegurar que la evidencia digital encontrada en la escena del crimen cumpla con las condiciones de admisibilidad descritas en la ley 527 de la constitución Colombiana [9]. Por ende, es necesario por parte de la persona o personas encargadas de realizar este paso tener en cuenta, entre otros, los siguientes aspectos:

- Escoger un método de recolección confiable con lo que se garantice la confiabilidad e integridad de la evidencia digital.
- Asegurar que los medios de almacenamiento donde se alojará toda la evidencia digital deben estar saneados[7].

[7] Garantizar que los dispositivos de almacenamiento utilizados para realizar las copias de la evidencia no hayan sido expuestas a ninguna variación magnética, óptica o similares [11]. El dispositivo debe haber sido formateado o saneado con alguna herramienta que funcione bajo

- Crear un registro con el que se inicia la cadena de custodia.
- Documentar de forma explícita cada interacción con la máquina víctima y la manipulación de la evidencia.

### *3.1.4. Escogencia de las herramientas para Windows XP de informática forense a usar durante la investigación (Paso 4)*

Al tener el computador a analizar y un posible vínculo con sus usuarios, se debe saber qué accesibilidad se tiene sobre los datos del equipo o disco(s) duro(s). Es por esto que dependiendo de la disponibilidad de los datos, cuentas de usuario en la máquina y las personas que interactúan con el computador, se debe determinar qué herramientas debe usar.

Para la selección de herramientas forenses a utilizar se debe listar las necesidades que se tienen, para acorde con ellas, asociar la herramienta adecuada. En esta guía se muestran algunas herramientas que soportan incidentes en Windows XP y otras dedicadas a sistemas de archivos NTFS[8] (Ver Anexo 1).

Luego de la escogencia, se debe redactar un documento con las herramientas seleccionadas y el por qué de su selección.

**ETAPA DE RECOLECCIÓN Y CLASIFICACIÓN DE INFORMACIÓN**

En esta etapa se pretende llevar a cabo el correcto procesamiento de las pruebas encontradas en la escena del crimen digital desde el momento en que se encuentran hasta que se llevan a un laboratorio para ser analizadas.

### *3.1.5. Tomar la hora que el sistema registra y la actual en caso tal que ambas difieran (Paso 5)*

---

el estándar que el Departamento de Defensa de los Estados Unidos sugiere (DoD 5220.22-M o National Industrial Security Program Operating Manual NISPOM).

[8] New Technology File System.

En el documento donde se está registrando todo lo relacionado con el caso, se debe especificar cuál es la hora que registra el sistema en el momento en que el equipo de respuesta a incidentes llegó a la escena y cuál es la hora local actual, con lo que se podrá observar si existe alguna diferencia, lo cual será de mucha utilidad para el paso 10 en donde se realizará una línea de tiempo.

### *3.1.6. Recolectar y tomar la imagen de los datos por orden de volatilidad y acorde con las propiedades del NTFS (Paso 6)*

Se busca recolectar y guardar la evidencia más frágil que son los datos volátiles, así que basándose en el orden de volatilidad mencionado en el Guidelines for Evidence Collection and Archiving (RFC3227), se inicia el proceso de recolección como se describe a continuación partiendo de lo más a lo menos volátil [5], [49].

### *3.1.7. Autenticación matemática de los datos (Paso 7)*

Para los datos recolectados en el paso anterior es necesario asegurar y garantizar que estos no se hayan modificado o alterado en la fase de recolección. Para esto se sugiere utilizar el algoritmo MD5, el SHA-1 u otros algoritmos que implementen funciones de Hash[9], el cual se debe realizar a cada imagen de datos no volátiles recolectada y almacenada para su posterior análisis.

### *3.1.8. Recolectar la información persistente (Paso 8)*

Con la información recolectada en el paso 6 a nivel de disco duro, se debe realizar una copia o las que se consideren necesarias de respaldo de las imágenes ya obtenidas, para luego ser analizadas en el laboratorio forense. Los datos originales deben mantenerse intactos, es decir, se debe trabajar sobre las imágenes y copias obtenidas de ellas [54].

[9] Es un valor numérico único de tamaño fijo que se utiliza para identificar archivos, carpetas, documentos o cualquier registro en un dispositivo de almacenamiento magnético.

Estas copias deben realizarse teniendo en cuenta las recomendaciones del paso 3 (Preservación de la Evidencia), y verificar que sean idénticas a la original. Es necesario que ésta verificación sea base en métodos matemáticos que manifiesten claramente la completitud de la información contenida en la copia. Para esto, es necesario apoyarse en software que implementes algoritmos de verificación, teniendo en cuenta que estas aplicaciones estén avaladas por las autoridades competentes en el caso [11].

**ETAPA DE ANÁLISIS DE EVIDENCIA**

Esta etapa se debe analizar la evidencia obtenida en los pasos anteriores. Juega un papel fundamental el analista en informática forense, al ser quien debe verificar la veracidad de lo encontrado anteriormente, dándole el uso adecuado a las herramientas forenses seleccionadas.

### *3.1.9. Clasificar la posible evidencia en orden cronológico (Paso 9)*

Este paso tiene como objetivo catalogar toda la evidencia recolectada en la escena del crimen según el orden cronológico proporcionado por los atributos MACE (Modificado, Accedido, Creado y Entrada modificada) de cada archivo involucrado. Esto con el fin de elaborar una secuencia y una línea de tiempo en la que se resumen las posibles acciones realizadas por el atacante.

Si se parte del hecho que se quiere profundizar en la aplicación de técnicas anti-forenses, es necesario analizar detenidamente la línea de tiempo; ya que es posible que el atacante manipule los atributos MACE para evitar que los archivos implicados en el ataque se clasifiquen en el orden cronológico, con lo que puede dificultar las acciones de los investigadores forenses.

Para evitar el escenario anterior y cumplir con el objetivo de este paso, el investigador encargado debe validar los siguientes aspectos:

- Indagar cuál fue la fecha y hora en la que la máquina atacada fue utilizada por última vez por su usuario.

- Luego de tener los registros de tiempo obtenidos en el enciso anterior, se debe relacionar estos con la actividad sospechosa en la máquina con el fin de relacionar cuáles acciones fueron hechas por el atacante y cuáles por el usuario del computador analizado.

- Analizar los datos obtenidos en el paso 2 (*Verificar que el contexto de la escena del crimen digital presente las características adecuadas*), específicamente en las entrevistas con el administrador del sistema y sus usuarios, para extraer cuáles son los horarios y días en la que comúnmente se utiliza la máquina víctima.

De acuerdo a la información obtenida del paso 2 (*Verificar que el contexto de la escena del crimen digital presente las características adecuadas*) y el 5 (*Tomar la hora que el sistema registra y la actual en caso tal que ambas difieran*), se deben analizar las acciones, procesos o archivos que se registren en días anteriores a los del incidente, para así comprobar si el atacante realizo algún proceso que le hubiese ayudado a preparar el ambiente adecuado para ejecutar el ataque. Cualquier evidencia de acciones sospechosas en este análisis debe ser anexada a la línea de tiempo.

Junto con la línea de tiempo establecida en este paso, se debe adjuntar un listado de los archivos sospechosos con el fin de delimitar la investigación para comenzar a hallar indicios de evidencia.

### *3.1.10. Determinar el estado y ubicación de la información encontrada (Paso 10)*

En este paso se busca que el especialista y analista en informática forense observe, analice y documente todo lo relacionado con la evidencia digital encontrada, utilizando los archivos que se clasificaron en el paso anterior como sospechosos o analizables, teniendo en cuenta los siguientes aspectos [49]:

- Ubicación de la información encontrada: documentando la dirección o path completo donde se encuentra la evidencia.

- Definir en qué medio de almacenamiento se encontró, es decir si la información está ubicada en discos duros, CD`s o memoria extraíbles entre otros.

- Definir, si es posible, el autor de la información, y el último usuario en accederla.

- Identificar cual fue el último evento en que estuvo involucrada esta información, así mismo, documentar el estado en el que se encontró, por ejemplo: eliminada, modificada o falsificada.

### *3.1.11. Clasificar la evidencia según el nivel de susceptibilidad de donde se pueden materializar las técnicas Anti-Forenses en un sistema operativo Windows XP SP3(Paso 11)*

Según lo define Cano [12], los niveles de susceptibilidad en los cuales las diferentes técnicas anti-forenses se pueden materializar independientemente del sistema operativo son: memoria, procesos, sistemas de archivos, aplicaciones y gestión de la inseguridad. A continuación se detalla con cada uno de los niveles los posibles rastros que se pueden dejar.

- Memoria: el principal indicio que muestre que una técnica anti-forenses fue realizada a nivel memoria, sería el de encontrar desbordamientos de pila (stack overflow). De igual forma, en caso tal que el computador atacado haya sido encontrado encendido y se haya recuperado los datos de la memoria cache, es importante revisarlos para observar si hubo copia, modificación o borrado de alguno de ellos.

- Procesos: usa como base los RootKits, los cuales pueden ser ejecutados en modo usuario o modo kernel, en el siguiente listado de métodos se tratan ambos. Para la detección de RootKits existen diferentes métodos, según lo plantea Hoglund y Butler [6], a continuación se enuncian los más comunes:

- ✓ Vigilando las puertas: se supervisan manualmente los rootkits en la medida en que se carguen en memoria desde el kernel o desde los procesos. Esto se logra al observar si librerías propias de Windows son cargadas en el momento de ejecutar una aplicación, sin embargo esto requiere de conocimientos de los rootkits y de las librerías que utiliza cada aplicación, aparte es un comportamiento no-determinista por los múltiples procesos que el sistema operativo utiliza que a su vez llaman librerías que pueden ser similares o las mismas de los rootkits.

- ✓ Escaneando las "habitaciones": al igual que el método descrito en el anterior enciso, éste también busca detectar el rootkit en su momento de carga en memoria, pero lo hace de una manera un poco más eficiente al escanear la memoria periódicamente buscando módulos o firmas de módulos usados por los rootkits.

- ✓ Buscando ganchos: consiste en encontrar los rootkits que se "enganchan" al kernel. Se busca encontrar las librerías DLL reemplazadas por otras que están "a favor" del rootkit, las cuales luego del cambio modifican código existente al ejecutarse las aplicaciones en ciertos casos. Las más severas se tienen cuando se toman servicios del kernel y se cambian valores de retorno de éstos para la actividad del rootkit. Dichos cambios se pueden encontrar de cinco maneras diferentes.

    - Enganchado la tabla de servicios (System Service Dispatch Table o KeServiceDescriptorTable)
    - Manejando la tabla de descripción de interrupciones(IDT)
    - Modificando la tabla de direcciones importadas (IAT)
    - Manipulando el manejador de paquetes de peticiones de drivers (IRP)

- Cambiando el código del kernel sus o apuntadores

✓ Seguimiento de ejecución: se basa en rastrear los procesos en el momento de ejecutarse, es decir, tomar cada proceso y sus respectivos hilos para determinar si un hilo hace llamado a otros procesos ocultos. Para su detección es necesario tomar las listas del sistema que manejan los hilos para realizar el seguimiento concerniente a cada proceso que los genera, es ahí en donde los rastros se pueden encontrar.

- Sistemas de archivos NTFS: toda evidencia que haya sido encontrada en el disco duro atacado, tiene cabida en este grupo.

- Aplicaciones: se observa cuando las aplicaciones hacen cosas indebidas, tienen comportamientos inusuales o fallan en determinados momentos. Las aplicaciones susceptibles a dichos problemas son por lo general las de código abierto o libre a las cuales se les puede estudiar y modificar sus estructuras para tomar control sobre ella. Por lo general, indicios de aplicaciones alteradas son aquellas que deniegan servicios de registro y autenticación, consumen altos porcentajes de memoria al ejecutarse o que sencillamente toman los archivos referentes o relacionados al software y los manipula a su gusto.

- Gestión de inseguridad: la evidencia ligada a este nivel se asocia con la ingeniería social realizada por personas dentro y fuera de la organización, las cuales buscan principalmente escalar ilegalmente permisos dentro de un sistema de información. Se puede detectar evidencia de este tipo cuando los comportamientos en las bases de datos o en los portales empresariales presentan anomalías en su funcionamiento y acceso. El acceso a “cookies” puede ser un gran objeto de estudio para esta evidencia.

### *3.1.12. Para la evidencia encontrada en el nivel de Sistema de Archivos, determinar la Técnica Anti-Forense posiblemente materializada (Paso 12)*

Basados en los distintos tipos de técnicas anti-forenses que son: destrucción, ocultación, eliminación y falsificación de la evidencia; en este paso se busca identificar el uso de cualquiera de estas técnicas en la ejecución del ataque.

Así que se debe revisar detenidamente la evidencia clasificada en el nivel de sistema de archivos por el paso 11, en busca de cualquier indicio de aplicación de algunos de los métodos mencionados anteriormente, teniendo como punto de partida la definición y objetivos de cada técnica anti - forense.

El analista en informática forense tiene como misión en este paso, efectuar las siguientes verificaciones según el tipo de técnica anti–forense evaluada:

#### *3.1.12.1. Obtención de información escondida u oculta (Paso 12.1)*

En este paso se inspecciona de una forma detallada el *slack space*. Proceso que se puede hacer mediante la ejecución de un *file carving* o búsquedas de *strings* [28], los campos reservados por el sistema de archivos, los sectores o *clusters* marcados como dañados en el sistema de archivos y toda la información oculta o protegida que se encuentre en particiones del disco duro [17].

A continuación se describe como realizar el análisis de algunos archivos específicos que podrán facilitar identificar si se aplicó la técnica anti – forense Ocultar Evidencia: [29]

a) Detección de datos ocultos en Cluster dañados:

- Verificar si existen cluster almacenados en el archivo $BadClus que estén marcados con el atributo $Bad, es decir que estén marcados como dañados; de ser así posiblemente haya datos escondidos en este lugar. Este archivo se encuentra en el segmento de disco número 8, asi que dirigiéndose a este lugar en

el disco y con la ayuda de un editor hexadecimal será posible realizar la verificación.

- Analizar detalladamente el contenido de estos cluster marcados como dañados (Bad) para encontrar cualquier indicio de información oculta.
- Extraer los Clusters sospechosos o que posiblemente tengan información oculta.
- Clasificar la información recogida como evidencia en el nivel de Ocultar evidencia.

b) Detección de datos ocultos en el $Boot File

- Extraer en $Boot File y el backup del Boot Sector que tiene almacenado por defecto el sistema de archivos NTFS de la imagen del disco duro que se tiene para el análisis forense.
- Realizar una comparación entre estos dos archivos para identificar si existe cualquier diferencia.
- Si existe cualquier diferencia entre estos archivos posiblemente exista datos ocultos, así que se debe realizar un análisis del contenido del $Boot File y de encontrar datos relevantes para la investigación serán clasificados en el nivel de Ocultar evidencia.

c) Detección de datos ocultos en el File Slack

- Obtener el número de sectores asignados en el sistema de archivos NTFS
- Calcular el número de espacios Slack que se encuentran en el disco duro, realizando la siguiente operación:

Slack Space=# Sectores asignados# Sectores por cada Cluster

- Si la operación anterior no es igual a cero, se analiza el contenido de estos Slack space.
- Si se encuentra información oculta en alguno de estos Slack space se clasifica en una tabla los datos encontrados.
- Definir o identificar conjuntos de datos relacionados o archivos divididos en varias secciones.

#### *3.1.12.2. Obtención de información borrada (Paso 12.2)*

En este proceso se busca cualquier información que el atacante no quisiera que fuera hallada por los investigadores forenses, así que cualquier información recuperada será clasificada en la evidencia que se analizará en pasos posteriores.

Teniendo en cuenta que los métodos de borrado de Windows no borran por completo los archivos o sus contenidos, es necesario revisar qué pasa con el espacio no asignado dentro de la partición NFTS [10]. En el momento en que estos métodos se invocan y se vacía la "papelera de reciclaje", muchos piensan que los archivos ya han sido borrados, pero la forma en que el NTFS funciona dice que sencillamente estos archivos se convierten en memoria no asignada al dejar de apuntar a ellos y el sistema operativo toma ese espacio como memoria disponible para ser asignada o sobre escrita. Es por esta razón, que es de suma importancia revisar por completo el espacio no asignado de la partición, ya que ahí se puede encontrar tanto archivos borrados, como espacio slack. Los datos siguen en el sitio original y con los mismos contenidos hasta el momento en que el sistema operativo decida sobrescribir en ese grupo de cluster con un nuevo archivo [76].

Por otro lado, al obtener la imagen del disco duro o partición NFTS, se debe analizar el archivo INFO2 el cual tiene un log de lo que se encuentra en la papelera con la fecha en la que fue "borrado" cada archivo y/o carpeta, la hora y su ubicación en disco entre otros. Este archivo estará disponible

siempre y cuando la papelera no se haya vaciado. Si la papelera ya ha sido vaciada, se debe revisar detalladamente el espacio no asignado mediante los encabezados y pie de páginas (footers) encontrados en éste en caso de poseerlos, de esta manera se podrá recuperar cualquier archivo borrado al desocupar la papelera de reciclaje. Otra forma de encontrar los archivos borrados es la revisión de la bandera IN_USE de los archivos en la MFT [22]. Sin embargo, los archivos recuperados en el espacio no asignado no se van a encontrar con atributos MACE ya que la entrada en la MFT se ha perdido al vaciar la papelera [76], se recomienda abrir el archivo y observar sus contenidos para tratar de encontrar alguna fecha en él que nos diga algo de su creación, modificación o último acceso.

Una situación que complica bastante la investigación es el uso de una herramienta de borrado seguro. Las herramientas básicas suelen llenar con ceros los *data units* ubicados en el *allocation bitmap* antes de poner el espacio como no asignado, lo que hace encontrar fácilmente los archivos "borrados" [15]. Sin embargo, no todas las herramientas de borrado seguro funcionan de esta manera básica y la consecución de ceros no es evidente. Si se tiene algo de información recolectada sobre el archivo borrado o se sospecha del uso de esta técnica, se debe realizar una revisión detallada a los siguientes elementos [22]:

- La MFT para ver si el archivo existió.
- El NTFS Journal para ver si existió en una partición NTFS.
- Cualquier backup del sistema.
- Espacio slack y no asignado para determinar si estuvo en el disco.

Si se conoce parte del archivo borrado de modo seguro, las tres primeras opciones pueden ayudar, de lo contrario y de estar el archivo sobre escrito es fundamental concentrarse en el espacio slack[10] o en el pagefile.

El mayor propósito de este paso es obtener palabras claves y compararlas con las ya encontradas del espacio slack asignado en los anteriores pasos. Juntando las palabras encontradas en los pasos anteriores y las del espacio no asignado, se debe crear una base de datos de palabras claves para la investigación. Se recomienda usar herramientas de búsqueda de texto para el análisis de esta base de datos. Luego de aplicar el software para búsqueda y análisis de texto, se debe revisar detalladamente las salidas que éste arroje para encontrar evidencia o patrones que lleven a ella.

#### *3.1.12.3. Identificación de información falsificada (Paso 12.3)*

Este proceso se basa en el análisis de metadatos, firmas de los archivos, identificación de cambio de extensiones o tipos de archivos o cambio de los atributos MACE; con el fin de determinar si el atacante ha manipulado archivos o información y de qué forma lo ha hecho.

Para el análisis detallado de la evidencia falsificada, se debe recurrir a MFT de la partición analizada. En la MTF se deben ubicar los atributos SIA (Standard Information Attribute) y FN (File Name Attribute) los cuales son los únicos que almacenan registros de tiempo de los archivos existentes [41] [40]. Con ellos de debe comparar ambos registros por cada archivo, ya que en condiciones normales, las fechas y horas registradas en SIA deben ser mayores o iguales a las registradas en FN.

#### *3.1.12.4. Identificación de la eliminación de fuentes de la evidencia (Paso 12.4)*

Se analizan las marcas de tiempo de los archivos que contienen los Log`s, al igual que el de eventos del sistema, con el fin de encontrar rangos de tiempo

[10] Teniendo en cuenta que todo archivo almacenado en disco utiliza varios clúster, el slack space se considera como el espacio dejado entre el último byte escrito y el siguiente clúster.

en los que estos registros no se almacenaron o generaron, lo que conlleva a los investigadores a subir la prioridad de análisis a los archivos o información manipulada en ese lapso de tiempo.

El proceso para este paso se describe a continuación:

- Ubicar los archivos generados por el Event Log de Windows.
- Realizar una línea de tiempo con estos archivos.
- Identificar si existen rangos de tiempo en los que no existe ningún log.
- Listar las fechas y horas en las que no existen log y compararla con el orden cronológico resultado del paso 9.
- De encontrar evidencia o acciones realizadas en las fechas y horas en la que no se registraron logs, se clasifica la evidencia en el nivel de eliminación de fuentes de la evidencia y se analiza su contenido.

### *3.1.13. Aplicar protocolos de informática forense para el análisis de la evidencia (Paso 13)*

En este momento, la investigación debe usar las herramientas de informática forense seleccionadas para el caso. Tomando cada una de ellas por sus características y analizando la evidencia encontrada para el sistema de archivos NTFS, se deben establecer todas las posibles relaciones entre la evidencia existente y sus gestores; se busca encontrar la mayor relación de eventos posible.

### *3.1.14. Clasificación de la evidencia (Paso 14)*

En este paso se divide la evidencia encontrada con base en la técnica forense que haya podido ser materializada según los resultados arrojados en el paso 13, con lo que se obtienen cuatro grupos de clasificación.

a) Destrucción de la evidencia.

b) Ocultar la evidencia.

c) Eliminación de las fuentes de la evidencia.

d) Falsificación de la evidencia.

Para la evidencia que presente indicios de aplicación de más de una técnica anti – forense, además de ser mencionada en los respectivos grupos, se registra en un matriz de correlación la cual contiene, el nombre o identificador de la evidencia y en orden cronológico los tipos de técnica anti -forense efectuadas por el atacante, esto con el objetivo de ir conformando una visión general de la secuencia de eventos que conformaron el ataque anti-forense.

### *3.1.15. Documentar la evidencia con indicios de aplicación de una técnica anti-forense (Paso 15)*

Con base al análisis de los pasos 13 y 14, se debe adjuntar un documento que muestre en forma detallada la evidencia que fue alterada, modificada o destruida luego de haberse considerado como prueba determinante y por ende si se va a considerar o no dentro del proceso de la investigación. Dicho documento se debe ir redactando conforme los incidentes se generan, incluyendo en él: quién realizó el procesamiento y las fechas y horas del suceso. También se debe mencionar el software forense utilizado para la gestión del incidente y los comandos o funciones que se emplearon. Es importante tomar pantallazos (screen shots) durante el proceso. Así mismo, se debe asegurar que las licencias del software comercial utilizado sean legales, ya que la defensa podría cuestionar la legalidad y confiabilidad de las aplicaciones [54].

**ETAPA FINAL**

### *3.1.16. Generación de reporte de resultados (Paso 16)*

Es el documento definitivo para la investigación, el líder del caso debe ser responsable de este reporte. En él, deben detallarse todos los hechos, hallazgos, elementos y evidencias que resultaron de toda la investigación, así como las relaciones con la escena del crimen, el posible sospechoso, la máquina víctima o con

el tiempo de utilización de cada elemento descrito en este reporte. Así mismo, se debe plasmar la documentación generada por las herramientas forenses seleccionadas para el caso, junto con su respectivo análisis y conclusiones.

# 4. VALIDACIÓN DE LA PROPUESTA

En esta sección se presentarán inicialmente cuatro ataques utilizando herramientas anti-forenses en escenarios reales. Estos escenarios incluyen redes alámbricas e inalámbricas de computadores conectados mediantes routers y switches en las que se cuenta con firewalls, anti-virus y la seguridad incluida con cada Windows XP SP3 junto con sus parches. Los cuatro ataques se dan con las siguientes herramientas:

1. TimeStomp: herramienta que modifica las estampillas de tiempo (timestamps) de cualquier archivo. Disponible en: http://www.metasploit.com/research/projects/antiforensics/

2. Slacker: aplicación la cual permite ocultar cualquier tipo de archivo en el espacio *Slack* de diferentes registros, para luego ser restaurados en el momento adecuado para realizar el ataque. Disponible en: http://www.metasploit.com/research/projects/antiforensics/

3. Evidence Eliminator: es el más avanzado en interfaz gráfica y con mayor funcionalidad de los tres, permite borrar de forma segura cualquier tipo de dato en un sistema de archivos NTFS. Disponible en: http://www.evidence-eliminator.com/

Con cada herramienta anti-forense se realizará el respectivo ataque, adicionalmente el último de los ataques es la conjugación de estas tres bajo el mismo escenario.

El detalle de la ejecución de los ataques que corresponden a los escenarios de prueba para la guía metodológica propuesta en este documento se encuentra en el Anexo 2.

## 4.1. Aplicación de la guía metodológica propuesta

En la búsqueda de proporcionar una herramienta útil para la informática forense que ayude en la identificación y validación de las técnicas anti-forenses, se realizó una aplicación de la guía

propuesta en esta investigación, utilizando un escenario de prueba (Contexto del ataque descrito en la sección anterior) en donde se aplicaron las técnicas que son objeto de estudio en este documento. Esto con el objetivo de retroalimentar la guía y reducir posibles brechas del resultado óptimo para un proceso de este tipo. El detalle de la aplicación se puede observar en el anexo 3.

A continuación se presenta los resultados que se obtuvieron al finalizar el análisis de la evidencia digital recolectada para el caso de estudio:

a. Como resultado del análisis de la línea del tiempo (Ver Anexo 3, ilustración 61) se evidencia que en el lapso de tiempo en el que ocurrió el ataque, se manipularon tres herramientas (slacker.exe, timestomp.exe y ee.exe) que otorgan funciones para la aplicación de técnicas forenses. Hecho que se tomó como primer indicio de la existencia de técnicas anti-forenses en el ataque.
b. Complementando la afirmación (a), se evidenció que las herramientas ya mencionadas se encuentran en estado de ejecución (Ver Anexo 3, Tabla 5).
c. Se concluye que efectivamente se ejecutó la herramienta anti-forense slacker.exe, sin embargo, no es posible encontrar evidencia de la información ocultada por esta herramienta, debido a que en el análisis del file slack no se hallaron datos.
d. Se observa un fuerte indicio del uso de la herramienta Evidence eliminator, como se describe en la sección 12.2 del anexo 3, en donde se encuentra evidencia de archivos e información utilizada por esta herramienta y en la que coincide su ultimo acceso con el rango de tiempo en el que se efectuó el ataque.
e. Se concluye que se aplicó la técnica anti-forense de falsificación de la evidencia, gracias al indicio que otorga el análisis de los atributos FN ($FILE_NAME Attribute) del archivo Nomina.xls (Ver Anexo 3, sección 12.3) y a lo mencionado en la afirmación (a) en donde se muestra el uso de la herramienta timestomp.exe.

Finalmente, con las afirmaciones que se realizaron, se puede evidenciar que los rastros e indicios que se dejan en un ataque que utilice técnicas anti-forenses, no son lo suficientemente claros y en muchos casos no concluyentes, abriendo el camino para dudas y ambigüedades en los resultados de una investigación forense. Por esta razón, se hace

necesario seguir estudiando estas técnicas y herramientas, para así poder ganarle la carrera a los que vulneran la seguridad informática.

# 5. RETROALIMENTACIÓN DE LA GUÍA METODOLÓGICA

Al finalizar la aplicación de la guía metodológica propuesta en el presente documento, surgen una serie de conclusiones y ajustes que ayudan a convertir esta guía en una herramienta eficiente para los investigadores forenses a la hora de validar la aplicación de técnicas anti-forenses. Las sugerencias y conclusiones que se aplicaron a la guía se listan a continuación.

- Debido a que esta guía metodológica busca ser parte de un protocolo para una investigación de informática forense, los pasos que se llevan a cabo en la etapa preliminar pueden ser homologados con la etapa inicial del protocolo escogido en la investigación. Esto con el objetivo de evitar realizar estos pasos en dos ocasiones.
- En la identificación y asignación de roles dependiendo del contexto de la investigación, es posible omitir algunos de ellos. Asimismo, es posible que un investigador sea responsable de varios roles a la vez, sino se cuenta con el recurso humano suficiente para suplir con la totalidad de roles necesarios en la investigación. Debe quedar documentado porque se decidió otorgar más de una responsabilidad a un investigador.
- En esta investigación se observó que además de los conocimiento profundos en informática forense, aspectos técnicos del sistema operativo involucrado, sistemas de archivos, entre otros, es de vital importancia los conocimientos de las características, funcionamientos y objetivos de las técnicas anti-forenses, debido a que en muchos de los casos éstas técnicas no proporcionan rastros claros y fáciles de encontrar. Además, las herramientas utilizadas para la investigación forense -que para este trabajo fue Autopsy-, no fueron diseñadas pensando en aplicación de técnicas anti-forenses.
- Herramientas como la línea de tiempo, proporcionan en la etapa de análisis de la evidencia una forma gráfica de correlacionar muchos de los eventos que al parecer están desvinculados en un ataque, ya que por las características mismas de las

técnicas anti-forenses, el rastreo y visualización es reducido. Por tal motivo, la correcta construcción de esta línea se convierte en un aspecto de alta prioridad en la investigación.

- Para el paso en el que se determina la técnica anti-forense que pudo ser materializada en el ataque (ver sección 3.1.12), se deben realizar una serie de operaciones que pueden llegar a ser un tanto complicadas; pero debido a que esta es una investigación académica en la que sólo se utilizó herramientas de código abierto, es posible que se obtengan unos mejores resultados y de una forma más fácil con herramientas que sean en mayor medida más especializadas, sofisticadas y robustas, como lo son las de licencias comerciales.

# 6. CONCLUSIONES Y TRABAJOS FUTUROS

## 6.1. Conclusiones

Luego de analizar los protocolos existentes de informática forense, se evidenció que ninguno de éstos contempla el uso de técnicas anti-forenses en un incidente de seguridad. Es por esto, que con este trabajo de grado se pretende complementar dichos protocolos, con el fin de obtener conclusiones más sólidas y concretas que guíen la investigación forense a generar resultados que se acerquen más a la realidad de los hechos ocurridos en un crimen informático. Para lograr esto, fue necesario realizar una recolección de información que abarca las diferentes variables en una investigación forense clásica, agregándole nuevas que se generaron al incluir las técnicas anti-forenses. De esta manera, se presenta una guía metodológica que incluye los dos conceptos ya mencionados, dentro de un modelo conceptual como lo es MoDeRaTA.

Luego de realizar la propuesta de la guía metodológica, se continuó el trabajo de grado con la validación de ésta al realizar un escenario de prueba en donde se realizaron ataques con herramientas anti-forenses. Los resultados a los que se llegaron fueron los siguientes:

- Con la validación que se realizó de la guía, se puede concluir que ésta se puede aplicar para investigaciones reales, teniendo en cuenta que al igual que se hizo con la

retroalimentación, es necesario realizar refinar el proceso a medida que se ejecuta cada uno de sus pasos.

- La amplia variedad de herramientas anti-forenses le dan una gran ventaja al atacante para realizar sus actos delictivos, ya que este tipo de aplicaciones han crecido y han evolucionado conforme Windows XP disminuye sus vulnerabilidades, es por esto que la guía se debe retroalimentar a medida surgen nuevas actualizaciones del sistema operativo ya mencionado.

- El Modelo Conceptual de Detección y Rastreo de Técnicas Anti-Forenses (MoDeRaTA), le permite a un grupo de investigadores forenses determinar la complejidad del caso a investigar, en la medida en que al encontrar el o los niveles de análisis vulnerados, pueden saber qué tanto conocimiento tiene el atacante y qué posibilidad hay de encontrar rastros del atacante. De esta manera, el modelo es un gran aporte a la planeación y determinación de recursos iniciales de una investigación forense. Para este caso en particular, el modelo se verificó con la aplicación de la guía en un nivel de análisis medio como lo es el de los sistemas de archivos, se encontraron rastros pero no todos los que debían encontrar, lo que sugiere que hay un grado de complejidad medianamente avanzado en los ataques, tal y como MoDeRaTA lo clasifica.

## 6.2. Trabajos Futuros

Después de culminar este trabajo de grado, se evidencian una serie de necesidades que debiera suplir la informática forense, para combatir las técnicas anti-forenses y así asegurar resultados más confiables. Por tal motivo, a continuación se describen los aspectos más relevantes en donde se genera un gran campo de investigación y análisis.

- Esta investigación está soportada en el Modelo Conceptual de Detección y Rastreo de Técnicas Anti-forenses (MoDeRaTA), enfocándose en el nivel de sistemas de

archivos. Sin embargo, este modelo cuenta con cuatro niveles más, que son: I) Gestión de (In) Seguridad, II) Aplicaciones, III) Procesos y IV) Memoria, en donde existe la necesidad de un análisis e investigaciones exhaustivas. En cada uno de estos niveles se necesita clasificar el tipo de técnicas que se pueden materializar, las distintas herramientas que existen en el mercado, las vulnerabilidades que explotan estas herramientas y el desarrollo de un proceso detallado para identificar la aplicación de alguna técnica anti-forense en cada nivel del modelo.

- Para efectos de delimitar la investigación, sólo se analizó el sistema operativo Windows XP Service Pack 3, con NTFS como sistema de archivos. De tal modo, se puede utilizar esta guía como plataforma para desarrollar nuevas investigaciones y análisis en máquinas que contengan los nuevos sistemas operativos Windows, como lo son Windows Vista, Windows 7 y los que estén por venir. Teniendo en cuenta que esta guía se basa en la versión 3.1 de NTFS, lo que coloca como restricción que los sistemas operativos que se analicen deben soportar esta versión de NTFS.
- Desarrollar investigaciones que estudien la aplicación de técnicas anti-forenses en los distintos sistemas operativos y diferentes sistemas de archivos, con lo se podría obtener resultados y características comunes, para así poder construir protocolos generales para la identificación de las técnicas anti-forenses y generar herramientas eficaces, confiables y eficientes para la informática forenses.
- Realizar estudios de las técnicas anti-forenses en otras áreas que pueden llegar a ser vulnerables a la aplicación de estas técnicas, como dispositivos de red, bases de datos, dispositivos móviles entre otros.

# 7. REFERENCIAS


[1] ABC-US Inc., "Must have software for any investigator", 2008, http://www.abcusinc.com/mm5/merchant.mvc?Screen=CTGY&Store_Code=AI&Category_Code=FSFT, Última consulta: 28/03/2009.

[2] Almanza, A, "Ciencias Anti-Forense: Un Nuevo Reto Para las Organizaciones", 2007, http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VII_JornadaSeguridad/VIIJNSI_AAlmanza.pdf, Última consulta: 20/07/2009.

[3] Ariza. A., Ruiz. J. "Análisis de Metadatos en archivos Office y Adobe", 2008, http://www.criptored.upm.es/guiateoria/gt_m142g1.htm, Última consulta: 28/03/2009.

[4] Botero, A., Camero, I., Cano, J. "Técnicas Anti-Forenses en Informática: Ingeniería Reversa Aplicada a Timestomp", 2009, http://www.criptored.upm.es/descarga/ActasCIBSI2009.zip, Última consulta: 02/02/2010.

[5] Brezinski. D., Killalea. T. "RFC 3227 – Guidelines for evidence collection and archiving", Febrero de 2002. http://www.faqs.org/rfcs/rfc3227.html, Última consulta: 02/05/2010.

[6] Butler, J., "Hoglund, G. Rootkits: Subverting the Windows Kernel", 22 de Julio de 2005, Addison Wesley Professional. ISBN: 0-321-29431-9, Última consulta: 11/01/2009.

[7] Cano, J. "Computación Forense: Conceptos Básicos", Mayo 2002, Última consulta: 23/02/2010.

[8] Cano, J. "Conceptos y retos en la atención de incidentes de Seguridad y la evidencia digital", Mayo del 2002, http://revistaing.uniandes.edu.co/pdf/rev15art9.pdf?ri=1551b155b1c040f2fd419e6e7fe10e5a, Última consulta: 10/09/2009.

[9] Cano, J. "Evidenia Digital: Reflexiones técnicas, administrativas y legales", 2004, http://www.urru.org/papers/RRfraude/DrJeimyCano.pdf, Última consulta: 05/06/2010.

[10] Cano, J. "Borrando Archivos, Conceptos básicos sobre la dinámica del funcionamiento de los sistemas de archivos", 2005, Última consulta: 11/02/2010.

[11] Cano, J. "Introducción a la informática forense: Una disciplina técnico – legal", 2006, http://www.acis.org.co/fileadmin/Revista_96/dos.pdf, Última consulta: 02/03/2009.

[12] Cano, J. "Introducción a las técnicas anti-forenses: conceptos e implicaciones para investigadores", Junio de 2007, http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VII_JornadaSeguridad/VIIJNSI_JCano.pdf, Última consulta: 05/10/2009.

[13] Cano, J. "Inseguridad Informática y Computación Anti-Forense: Dos Conceptos Emergentes de la Seguridad de la Información", 2007, http://www.virusprot.com/Archivos/Antifore07.pdf, Última consulta: 07/01/2010.

[14] Cano, J. "Computación Forense: Descubriendo los rastros informáticos", 2009, México: Alfaomega, ISBN 978-958-682-767-6, Última consulta: 09/09/2010.

[15] Carrier, B. "File System Forensic Analysis", 17 de marzo de 2005, Addison Weasley Professional, ISBN 0-32-126817-2, Última consulta: 10/12/2010.

[16] Computer Forensics, Cybercrime and Steganography Resources, "Computer Forensic Toolkits, Digital Evidence Software Suite", Junio de 2009, http://www.forensix.org/toolkits, Última consulta: 08/07/2010.

[17] Córdoba, J., Laverde, R., Ortiz, D., Puentes, D. "Análisis de Datos: Una propuesta metodológica y su aplicación en The Sleuth Kit y EnCase", Octubre de 2005, http://www.criptored.upm.es/guiateoria/gt_m142y.htm, Última consulta: 02/18/2010.

[18] Consejo Nacional de la Policía Judicial, "Manual Único de la Policía Judicial", Mayo de 2005, http://www.fiscalia.gov.co/sistpenal/sistemapenal/manualpolicia.pdf, Última consulta: 04/01/2010.

[19] Coria, P. "Introducción a la criminalística de campo y de laboratorio", 16 de Diciembre de 2008, http://www.cienciaforense.cl/csi, Última consulta: 05/21/2009.

[20] Cybex, the Digital Forensic Company. "Prevención, detección e investigación del fraude en entornos virtuales". 2008, http://www.cybex.es/es/servicios_herramientas.htm, Última consulta: 05/20/2009.

[21] Digging Inn. "NTFS Time Stamps", 2008, http://blogs.technet.com/ganand/archive/2008/02/19/ntfs-time-stamps-file-created-in-1601-modified-in-1801-and-accessed-in-2008.aspx, Última consulta: 20/02/2010.

[22] Davis, C., Philip, A., Cowen, D. "Hacking Exposed: Computer Forensics Secrets and Solutions", 22 de noviembre de 2004, McGraw Hill/Osborne, ISBN 0-07-225675-3, Última consulta: 09/02/2010.

[23] Eddy, W. "RCF 4987 TCP SYN Flooding Attacks and Common Mitigations", 2007, http://tools.ietf.org/html/rfc4987, Última consulta: 08/10/2010.

[24] e-fence, "Cyber Security and Computer Forensics Software. Helix 3", 2009, http://www.e-fense.com/h3-enterprise.php, Última consulta: 20/02/2010.

[25] The Ethical Hacker Network, "The Metasploit Anti Forensic Investigation Arsenal MAFIA", 2010, http://www.ethicalhacker.net/component/option,com_smf/Itemid,54/topic,5450.msg28383/topicseen,1/, Última consulta: 02/02/2010.

[26] Fierro, H. "Introducción a la Criminalística", 2006, Ed. Leyer, Última consulta: 05/05/2009.

[27] Harris, R. "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem", 2006, http:// dfrws.org/2006/proceedings/6-harris.pdf, Última consulta: 05/05/2009.

[28] Heredia, T. "Gestión y tratamiento de incidentes de seguridad de la información, Parte 3: Recolección y análisis de información", Julio de 2008, http://www.arcert.gov.ar/ncursos/material/gestion_de_incidentes-parte_3-v2.1.1-6pp.pdf, Última consulta: 28/01/2010.

[29] Huebner, E., Bem, D., KaiWee, C. "Data hiding in the NTFS file system", Octubre de 2006, http://www.sciencedirect.com/, Última consulta: 27/05/2009.

[30] Info Seguridad, "Esteganografía", 2008, http://www.infoseguridad0.es/Estenografia.htm, Última consulta: 29/05/2009.

[31] IOCE, "Guidelines For Best Practice In The Forensic Examination Of Digital Technology", 2002, http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html, Última consulta: 17/04/2009.

[32] Jess, P. "Session Hijacking in Windows Networks. 2006", http://www.sans.org/reading_room/whitepapers/windows/session-hijacking-windows-, networks_2124, Última consulta: 12/07/2010.

[33] Liberaria Tempus, "Borrado Seguro de Ficheros", 2009, http://www.liberaliatempus.com/secure-delete.html, Última consulta: 14/07/2010.

[34] López, O., Amaya, H., León R., Acosta B. "Informática Forense: Generalidades, aspectos técnicos y herramientas", 2002, http://www.criptored.upm.es/guiateoria/gt_m180b.htm, Última consulta: 19/04/2009.

[35] Kozierok. C. "NTFS Architecture and Structures", 2010, http://www.pcguide.com/ref/hdd/file/ntfs/arch.htm, Última consulta: 23/10/2009.

[36] Kozierok. C. "NTFS System Metadata Files", 2010, http://www.pcguide.com/ref/hdd/file/ntfs/archFiles-c.html, Última consulta: 22/10/2009.

[37] Kozierok. C. "NTFS Directories and Files", http://www.pcguide.com/ref/hdd/file/ntfs/files_Attr.htm, Última consulta: 22/10/2009.

[38] Liu, V. "Metasploit Anti-Forensics Project", 2008, http://www.metasploit.com/data/antiforensics/BlueHat-Metasploit_AntiForensics.ppt, Última consulta: 20/05/2009.

[39] Metasploit. "Administracion de registros", 2009, http://www.metasploit-es.com.ar/wiki/index.php/Administraci%C3%B3n_de_registros, Última consulta: 28/05/2009.

[40] MicrosoftTechNet, "How NTFS Works", 28 de marzo de 2003, http://technet.microsoft.com/en-us/library/cc781134.aspx, Última consulta: 22/10/2009.

[41] MicrosoftTechNet. "NTFS TimeStamps", 2008, http://blogs.technet.com/ganand/archive/2008/02/19/ntfs-time-stamps-file-created-in-1601-modified-in-1801-and-accessed-in-2008.aspx, Última consulta: 22/10/2009.

[42] Microsoft Corporation, "How NTFS Works", 2008, http://technet.microsoft.com/en-us/library/cc781134.aspx, Última consulta: 23/10/2009.

[43] MicrosoftTechNet, "File Systems", 2010, http://technet.microsoft.com/en-us/library/cc766145%28WS.10%29.aspx, Última consulta: 14/08/2010.

[44] Microsoft Developer Network, "Using Event Log", 2010, http://msdn.microsoft.com/en-us/library/aa385772v=VS.85.aspx, Última consulta: 26/09/2010.

[45] National Industry Security Program, Department of Defense, "National Industry Security Program Operations Manual", 1997, http://www.usaid.gov/policy/ads/500/d522022m.pdf, Última consulta: 02/10/2010.

[46] National Institute of Standards and Technology, "An Introduction to Computer Security: The NIST Handbook", Octubre de 1995, http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf, Última consulta: 02/10/2010.

[47] National Justice Institute, "Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition", Abril de 2008, http://www.ncjrs.gov/pdffiles1/nij/219941.pdf, Última consulta: 21/08/2010.

[48] National Justice Institute, "Guide to Integrating Forensic Techniques into Incident Response", Agosto del 2006, http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf, Última consulta: 19/05/2009.

[49] Nolan. R., O´Colin. S., Branson. J., Waits. C., "First Responders Guide to Computer Forensics", Marzo de 2005, www.cert.org/archive/pdf/FRGCF_v1.3.pdf, Última consulta: 10/08/2010.

[50] Noblett, M., Pollitt M., Presley A. "Recovering and Examining Computer Forensic Evidence", 2000, http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm, , Última consulta: 11/07/2010.

[51] Ntfs.com. "NTFS Basics", 2008, http://www.ntfs.com/ntfs_basics.htm, Última consulta: 20/08/2009.

[52] Ntfs.com, "Partition Boot Sector", 2008, http://www.ntfs.com/ntfs-partition-boot-sector.htm, Última consulta: 21/08/2009.

[53] New Technologies Inc. "Windows NT Forensic Utility Suite", 18 de enero de 2004, http://www.forensics-intl.com/suite9.html, Última consulta: 21/08/2009.

[54] New Technologies Inc. "Computer evidence processing guidelines", 2005, http://www.forensics-intl.com/evidguid.html, Última consulta: 21/08/2009.

[55] Olney, Matthew; Grenier, Lurene; Zidouemba, Alain. "ms08_067 Sourcefire Vulnerability Research Team Report". Octubre de 2008, http://pentest.cryptocity.net/files/exploitation/ms08-067wp.pdf, Última consulta: 01/08/2010.

[56] PC In One, "File Systems Unraveled", 2010, http://www.pcnineoneone.com/howto/filesystems1.html, Última consulta: 21/08/2009.

[57] Ramírez, R. "El principio de intercambio", 18 de mayo de 2004, http://www.chasethesun.es/docs/locard.pdf, Última consulta: 13/09/2010.

[58] Russon, R. "NTFS Documentation", 2009, http://inform.pucp.edu.pe/~inf232/Ntfs/ntfs_doc_v0.5/index.html, Última consulta: 21/08/2009.

[59] Saferstein, R. "Criminalistics: An Introduction to Forensic Science", 31 de Julio de 2000, Ed. Prentice Hall, Última consulta: 18/05/2009.

[60] Standards Australia International, "HB 171-2003 Guidelines for the management of IT Evidence", 2003, Última consulta: 11/08/2010.

[61] Sammes, T, Jeninson B, "Forensic Computing A Practitioners Guide", 2nd. ed, 2007, , Última consulta: 20/09/2010.

[62] StegoArchive. "What is Steganography?", 2005, http://members.cox.net/ebmmd/stego/stego.html, Última consulta: 09/08/2009.

[63] Skape, "Metasploit's Meterpreter", Diciembre de 2004, http://www.nologin.org/Downloads/Papers/meterpreter.pdf, Última consulta: 02/08/2009.

[64] Spam, Spam. "Glosario de términos, con definiciones acerca de palabras relacionadas con la seguridad informática", 2010, http://www.spamspam.info/glosario/, , Última consulta: 12/10/2010.

[65] Microsoft Support. "Descripción de las características de Plug and Play universal en Windows XP", 2007, http://support.microsoft.com/kb/323713/es, Última consulta: 03/07/2010.

[66] Microsoft Support. "Cómo ver y administrar registros de sucesos en el Visor de sucesos de Windows XP?", 2010, http://support.microsoft.com/kb/308427, Última consulta: 09/08/2010.

[67] Microsoft Support. "Introducción a los Sistemas de archivos FAT, HPFS y NTFS", 2008, http://support.microsoft.com/kb/100108/es, Última consulta: 21/08/2009.

[68] Tech Development Co. "NTFS file system manages - NTFS file system metafiles", 2008, http://www.easeus.com/data-recovery-ebook/ntfs-file-system-metafiles.htm, Última consulta: 21/08/2009.

[69] Tech market, "Reparse Points", 2010, http://msdn.microsoft.com/en-us/library/aa365503VS.85.aspx, Última consulta: 10/08/2010.

[70] The Free Country. "Free Secure Destructive File and Disk Deletion Tools", 2010, http://www.thefreecountry.com/security/securedelete.shtml, Última consulta: 23/09/2010.

[71] Microsoft Technet. "Windows XP Technical Overview", 2007, http://technet.microsoft.com/en-us/library/bb457060.aspx, Última consulta: 15/10/2010.

[72] Tu, Y. "NTFS File System and Data Security", 2006. http://xcon.xfocus.org/XCon2006/archieves/Yanhui_Tu-NTFS_File_System_Kernel_Analysis_and_Database_Security.pdf, Última consulta: 16/06/2010.

[73] Valencia, M., Acosta M., Jaimes G., Reyes I., Valencia J., Jiménez J., Bermúdez J., Díaz M., Devia F. Fiscalía General de la Nación, "Manual de Procedimientos del Sistema de Cadena de Custodia", 2006, http://www.usergioarboleda.edu.co/derecho_penal/2004MANUAL%20CADENA%20DE%20CUSTODIA.pdf, Última consulta: 24/08/2010.

[74] Vásquez. C. "METADATOS: Introducción e historia", 2001. http://www.dcc.uchile.cl/~cvasquez/introehistoria.pdf, Última consulta: 12/09/2009.

[75] Vásquez, G., Valero, C., Jiménez, M., Puentes, I., Camacho, E., Guzmán, J. "Tecnología en Criminalística IV Periodo", 2006, ISBN 958.33.8831, Última consulta: 07/05/2009.

[76] White, P. "Crime Scene Court: the essentials of forensic science", 2004, UK: the Royal Society of Chemistry, ISBN 0-854054-656-9, Última consulta: 11/08/2010.

[77] Web Statistics and Trends. "OS Platform Statistics", 2009, http://www.w3schools.com/browsers/browsers_os.asp, Última consulta: 10/08/2010.

[78] X-Ways Software Technology AG. "X-Ways Forensics – an advanced computer examination and data recovery software", 2007, http://www.x-ways.net/winhex/forensics.html, Última consulta: 29/05/2009.

[79] Microsoft Co. "Overview of Windows XP Service Pack 3", 2008, http://download.microsoft.com/download/6/8/7/687484ed-8174-496d-8db9-f02b40c12982/overview%20of%20windows%20xp%20service%20pack%203.pdf, Última consulta: 17/10/2010.

[80] Cano, J. "Técnicas en Informática Forense", 2010, http://auditor2006.comunidadcoomeva.com/blog/uploads/informaticaforense.pdf, Última consulta: 11/05/2009.

[81] KSHETRI, N. (2006) The simple economics of cybercrime. IEEE Security & Privacy. January/February. SUNDT, C. (2006) Information security and the law. Information Security Technical Report. Vol.2 No.9, Última consulta: 07/08/2010.