



# DIGITAL FORENSICS -AN INTRODUCTION

## Tabla de contenido

Abstracto	3
Elementos de un crimen	4
Objetivos de un examinador forense digital	5
Clasificación de la ciencia forense digital	6
Evidencia Digital	7
Comprensión de datos y metadatos	8
Principios de la ciencia forense digital	9
Proceso de Investigación Forense Digital	10
Tipos de herramientas	11
Diferencia entre E-discovery y análisis forense digital	12
• Descubrimiento electrónico	12
• Forense digital	12
Metodología para el Investigador del DF	13
Métodos de recopilación de pruebas	15
Imagen de disco y clonación	dieciséis
Desafíos que enfrenta el investigador del DF	17
Ventajas de la ciencia forense digital	18
Contras de la ciencia forense digital	18
Conclusión	18
Referencias	18
Sobre nosotros	19

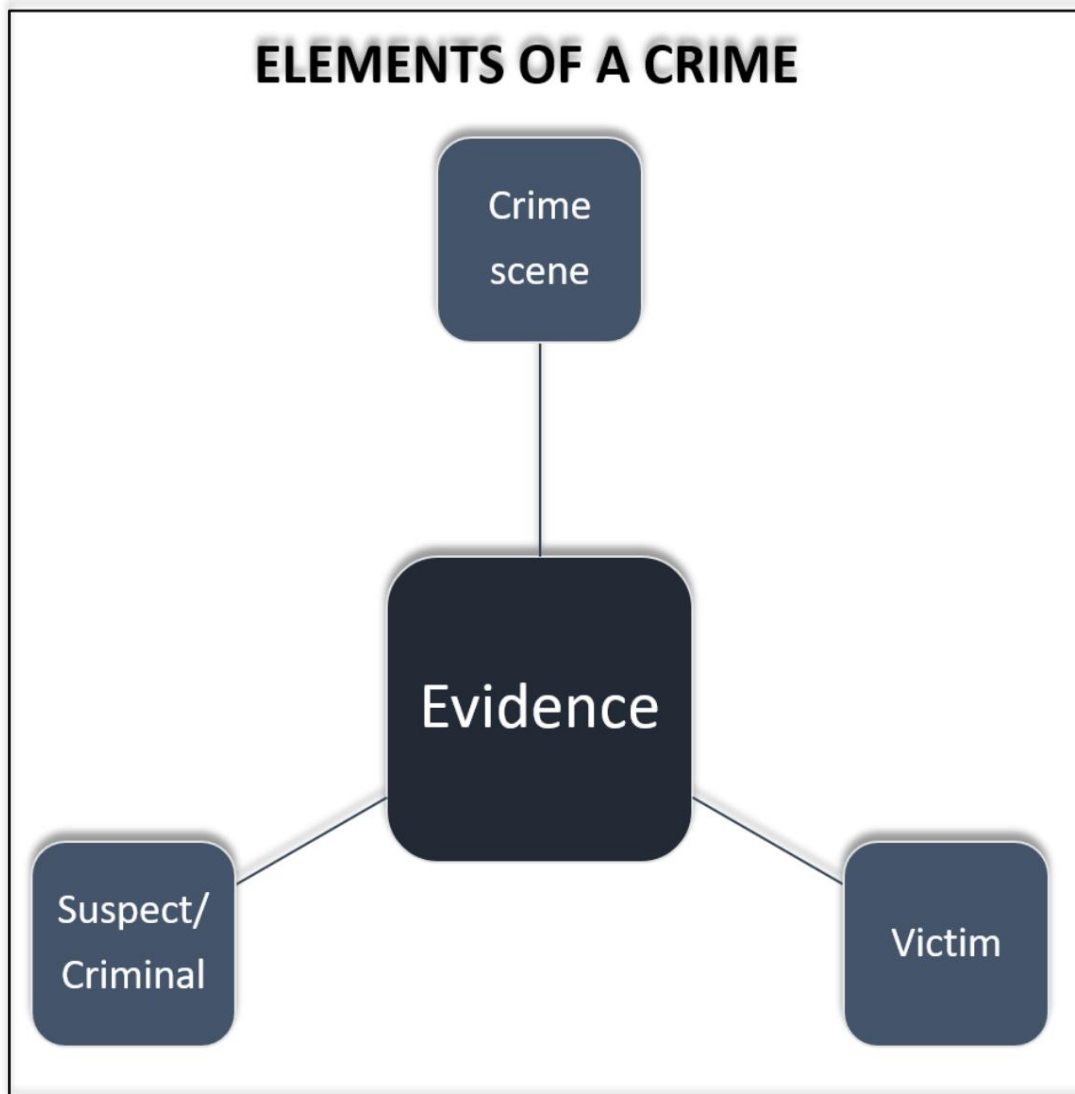
## Abstracto

Hay situaciones en las que un individuo o una organización pueden ser víctimas de un ciberataque y quizás te preguntes cuál es la forma correcta de proceder. Una investigación forense digital exhaustiva puede cerrar la investigación de estos ataques. En este artículo, aprenderemos sobre los fundamentos de la ciencia forense digital.

La ciencia forense digital es la aplicación de métodos científicos para preservar, recuperar e investigar evidencia digital en un escenario de delito digital. Se puede definir correctamente como recopilación, examen, análisis y documentación mediante el uso de métodos científicamente probados para investigar un delito digital y presentarlo ante el tribunal.

## Elementos de un crimen

Para probar un delito digital, como investigador debes contar con los siguientes elementos para llegar a una conclusión. Todos los elementos estarán relacionados entre sí más o menos.



En el año 1978 se reconoció el primer delito informático en la Ley de Delitos Informáticos de Florida.



## Objetivos de un examinador forense digital

Como investigador forense digital, debe tener un objetivo de investigación. A continuación se describen los cinco objetivos más importantes de la investigación:



El principal tratado internacional europeo, la Convención sobre Ciberdelincuencia, entró en vigor en 2004

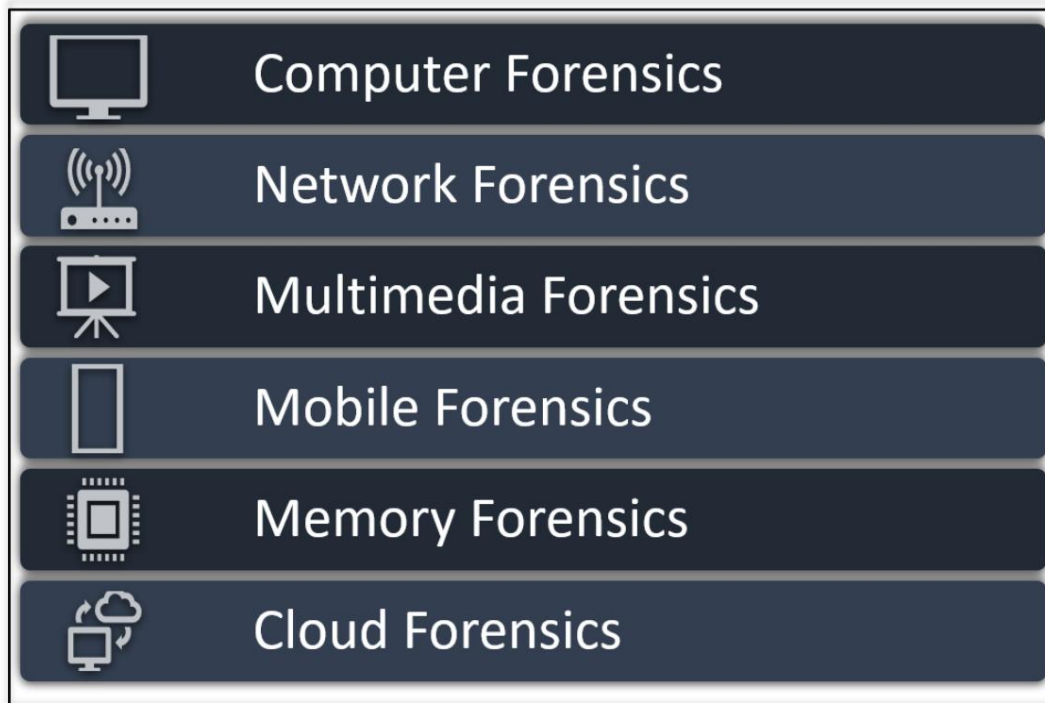


## Clasificación de la ciencia forense digital

La ciencia forense digital es un término muy amplio que tiene varias clasificaciones dentro del mismo. Las investigaciones forenses más populares son las siguientes:

1. **Computación forense:** es el tipo más primitivo de ciencia forense digital que generalmente se introdujo en la evolución temprana de los sistemas informáticos. Incluye la investigación de computadoras, portátiles, registros, unidades USB, discos duros, sistemas operativos, etc.
2. **Análisis forense de redes:** incluye la investigación mediante el análisis de eventos, intrusiones y datos de la red. paquetes que se transmitieron para detectar ataques a la red.
3. **Análisis forense multimedia:** comprende la investigación de archivos de imágenes, audio y video que se encuentran recuperado como evidencia en la escena de un crimen digital.
4. **Análisis forense móvil:** comprende la investigación de teléfonos inteligentes como Android, iOS, etc. para encontrar evidencia digital y recuperar los datos eliminados importantes para el caso.
5. **Análisis forense de la memoria:** es la investigación forense de la memoria o volcado de RAM del sistema para descubrir la memoria volátil como el historial de chat, el historial del portapapeles, el historial del navegador, etc.
6. **Análisis forense de la nube:** teniendo en cuenta que el almacenamiento virtual tiene demanda, la investigación del entorno de la nube también desempeña un papel clave en la escena del crimen digital para recopilar pruebas.

La clasificación de la ciencia forense digital no se limita al diagrama anterior y se puede clasificar en más según los casos.



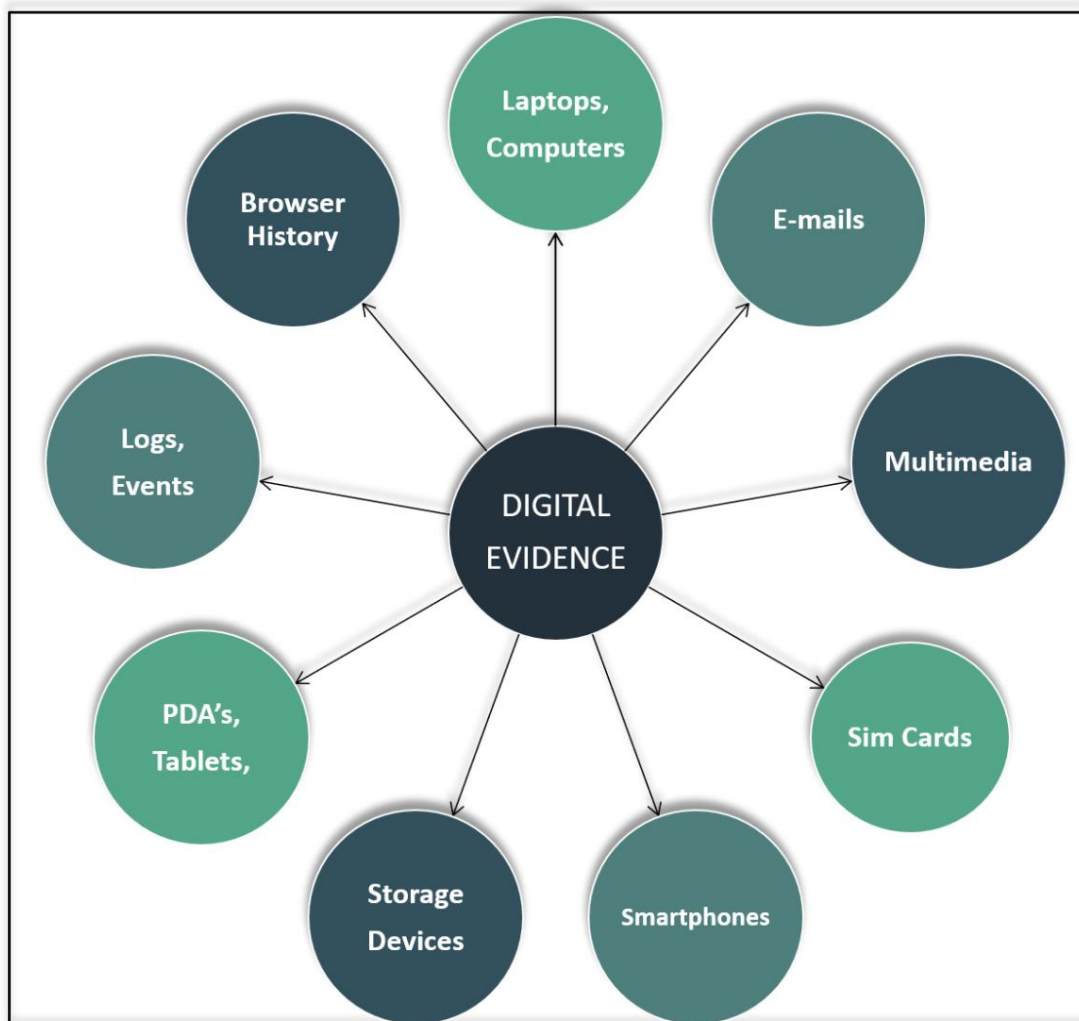
# Evidencia Digital

La evidencia digital o evidencia electrónica se puede definir como cualquier objeto que almacene información digital y la transmita en cualquier forma que haya sido utilizada en el acto del delito o en apoyo a la investigación del caso en un juicio ante el tribunal.

La evidencia encontrada en la escena del crimen debe tener dos propiedades clave

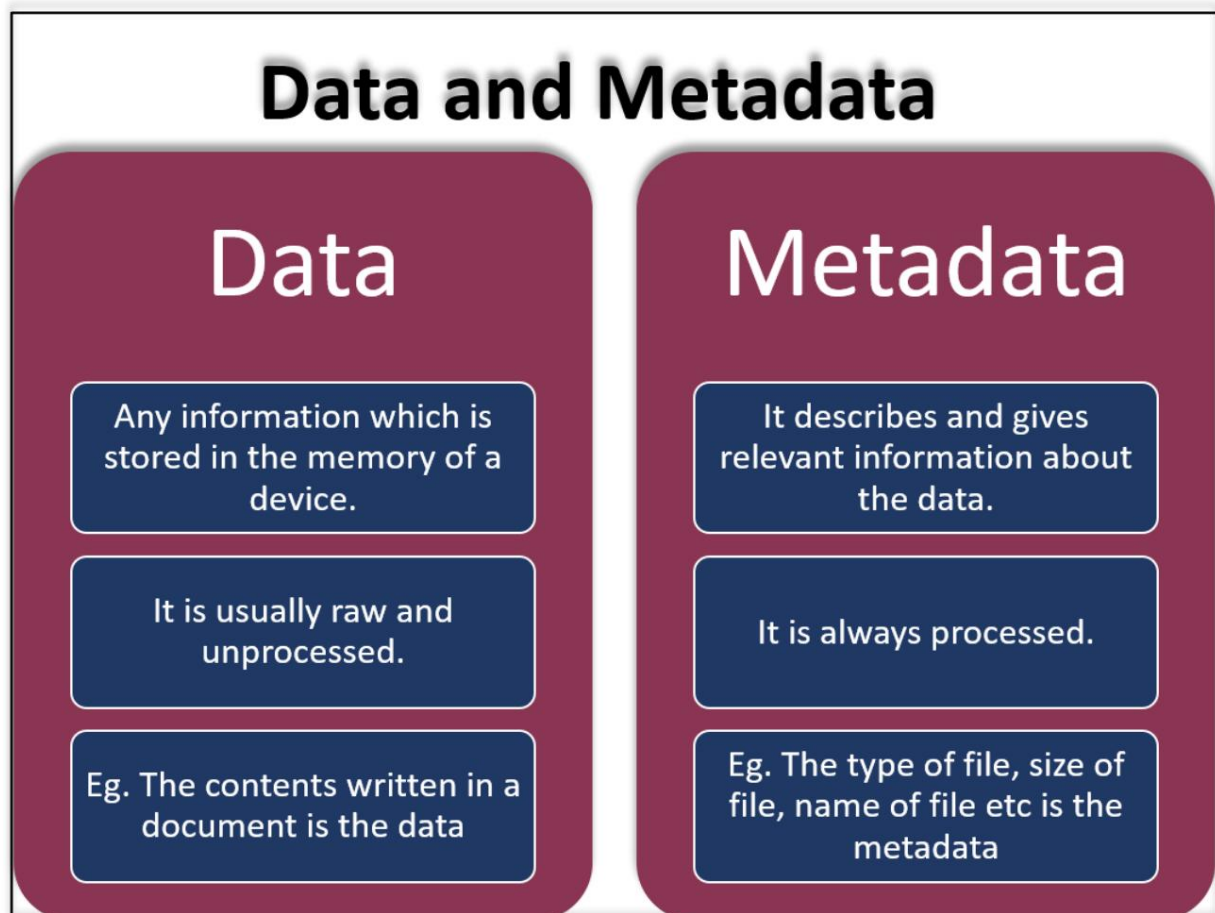
- a. Deberían ser admisibles en el tribunal.
- b. Deberían ser auténticos.

La evidencia digital puede ser de varios tipos y debe aprovecharse de manera ética siguiendo las pautas prescritas de investigación. Aquí hay algunos ejemplos digitales de evidencia en el diagrama a continuación, pero la lista continúa.



## Comprensión de datos y metadatos

La diferencia entre los datos y los metadatos para la investigación forense se puede entender fácilmente con la ayuda del siguiente diagrama:



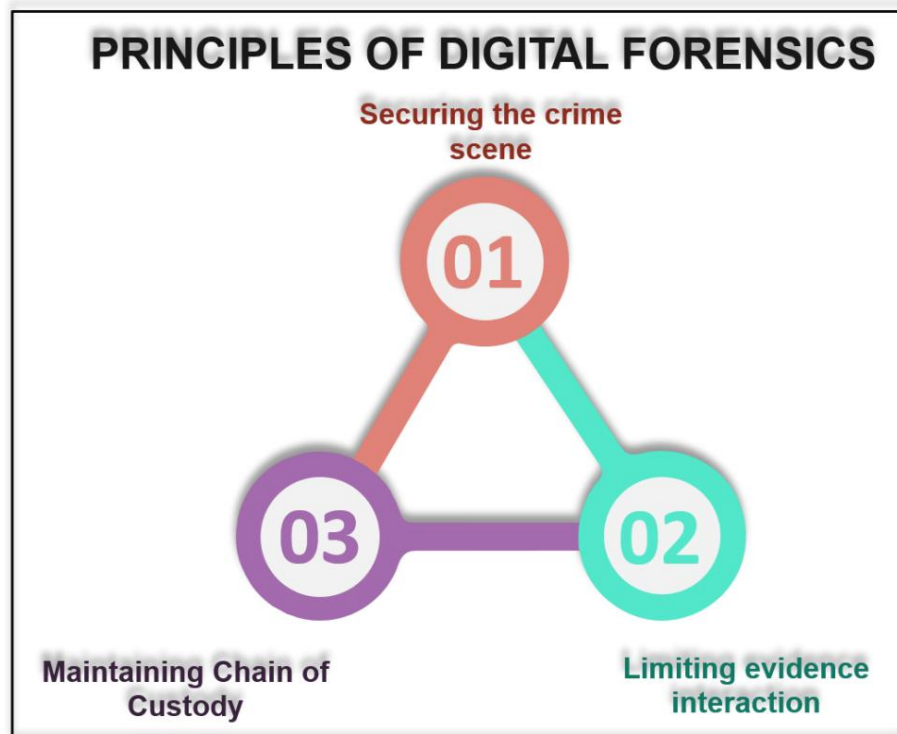
Los metadatos a menudo se definen como datos dentro de datos.





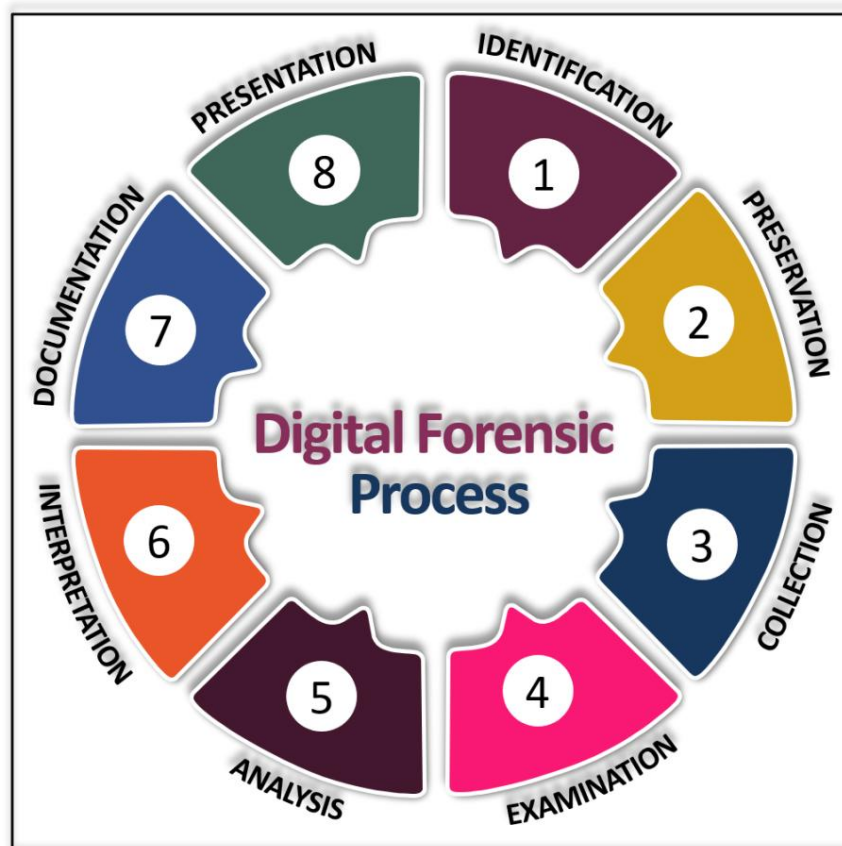
## Principios de la ciencia forense digital

1. **Proteger la escena del crimen:** este es el principio más importante de la ciencia forense digital. Como investigador, debe prohibir cualquier acceso a su evidencia digital sospechosa, documentar todos los procesos y conexiones, desconectar las conexiones inalámbricas, etc. para conservar su evidencia. seguro.
2. **Limitación de la interacción con la evidencia:** como investigador, debe asegurarse de que su evidencia tenga una interacción limitada al capturar el RAM y también pueda realizar ataques de arranque en frío sobre la evidencia.
3. **Mantenimiento de la cadena de custodia:** La cadena de custodia es un registro de la secuencia en la que se recopiló la evidencia, la fecha y hora de la recolección, el investigador que accedió a ella y la manejó, etc.



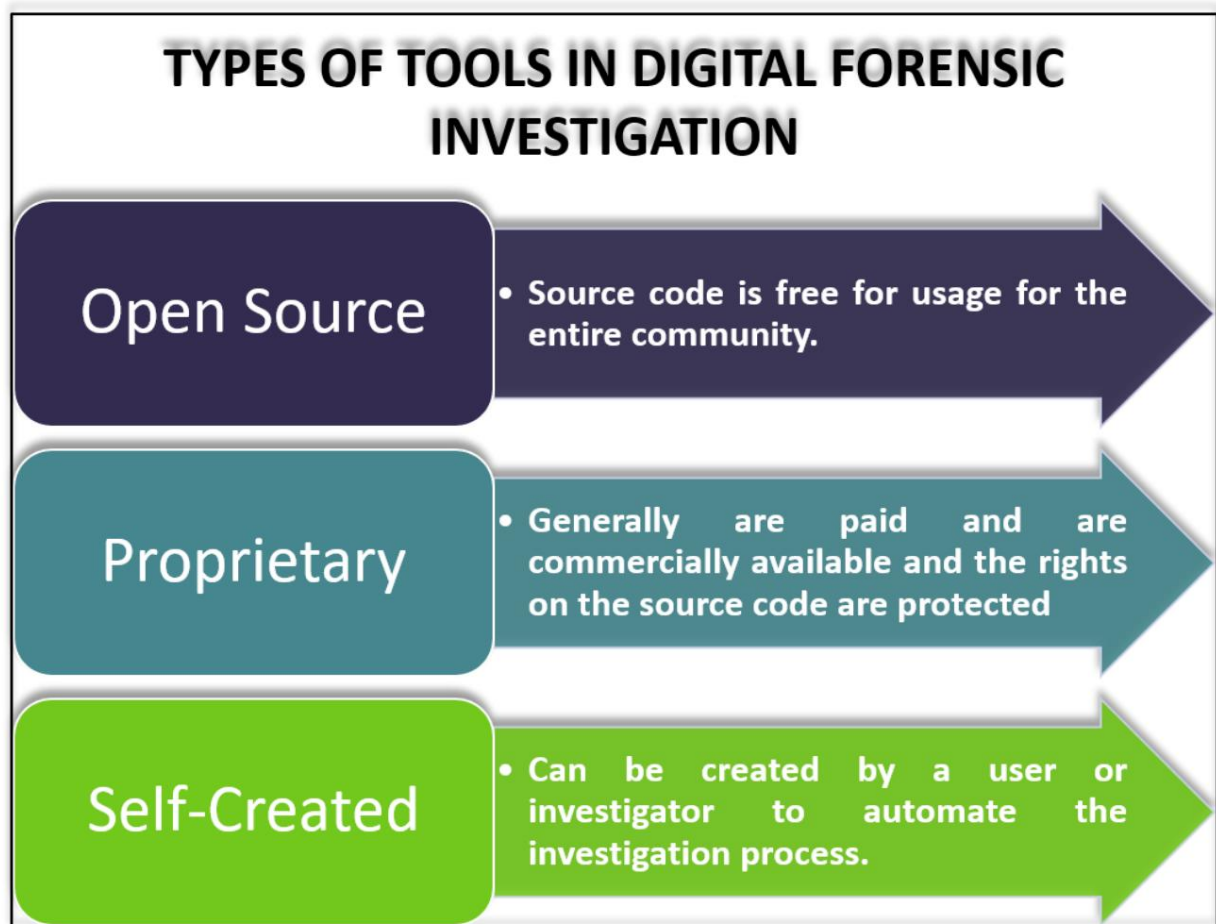
# Proceso de Investigación Forense Digital

- **Identificación:** Este es el primer paso que da un investigador en la escena del crimen para identificar el propósito de la investigación y reconocer la posible evidencia digital.
- **Preservación:** este es el siguiente paso en el que el investigador debe tener cuidado ya que debe asegurarse de que la evidencia no haya sido alterada, lo que puede complicar la investigación.
- **Recopilación:** este paso implica adquirir la evidencia más apropiada sin causando cualquier daño a la evidencia y empaquetándola en una Bolsa de Faraday.
- **Examen:** Este paso es previo a la realización de cualquier análisis de la evidencia. Este paso requiere una inspección cuidadosa de la evidencia en busca de otros detalles secundarios.
- **Análisis:** En este paso, el investigador lleva a cabo las cosas más cruciales como unir los fragmentos de las pruebas, recuperar archivos eliminados, etc.
- **Interpretación:** Este paso implica concluir el hallazgo de la investigación después reconstrucción de la escena del crimen.
- **Documentación:** este paso suele implicar la preparación de un informe detallado o un documento sobre toda la investigación.
- **Presentación:** Este es un paso obligatorio sólo cuando se solicita un contrainterrogatorio que debe mencionarse en términos muy simples de comprensión para los plebeyos.



## Tipos de herramientas

Un investigador debe tener el conjunto de herramientas adecuado para realizar una investigación forense digital. Corresponde al investigador decidir la herramienta adecuada para el caso. Las herramientas también dependen de la aplicación basada en hardware y software. Los tipos de herramientas se pueden clasificar en tres tipos; Código abierto, propietario y de creación propia.



## Diferencia entre descubrimiento electrónico y digital forense

La comunidad de Internet muchas veces se confunde entre estos dos términos. Aquí algunos puntos que resaltar la importancia y el uso del descubrimiento electrónico y la ciencia forense digital.





### descubrimiento electrónico

E-Discovery significa descubrimiento electrónico. Puede definirse como el proceso involucrado en la recopilación, preparación, revisión, interpretación y presentación de documentos electrónicos de discos duros y otras formas de dispositivos de almacenamiento en litigios civiles. Los siguientes son los puntos clave para recordar en E-discovery.

E-DISCOVERY	
	Useful in Civil Litigations
	Does not involve erased data
	Focuses on data in Allocated Spaces
	Limited Data Recovery
	Testimony is based on Facts

### Forense digital

La ciencia forense digital se puede definir como el proceso de preservación, identificación, extracción y documentación de evidencia digital que utiliza el tribunal de justicia para facilitar las investigaciones criminales.

DIGITAL FORENSICS	
	Useful in Criminal Investigation
	Deleted Data can be recovered
	Focuses on data in Unallocated Spaces as well
	Finding of data is unrestricted
	Testimony is based on Digital Forensic Expert

# Metodología para el Investigador del DF

Un investigador forense digital tiene una gran responsabilidad sobre sus hombros cuando investiga un caso, ya que sus hallazgos harán justicia a los inocentes y castigarán al criminal. Por tanto, existe una serie de pasos que debe seguir cuando investiga un caso. Los siguientes son un paso generalizado de la investigación, mientras que el Investigador puede seguir los pasos prescritos por su Institución o el marco que sigue.

**PASO 01: Prepare un diseño preliminar o un método para abordar el caso.** El investigador debe preparar un método sobre cómo realizará la investigación y tener una comprensión clara de la escena del crimen.

Debe asegurarse de que en una escena donde la computadora o un dispositivo esté encendido, no debe cometer el error de apagarlo, ejecutar ningún programa o realizar cualquier otra actividad.

**PASO 02: Determinar los recursos que se requieren para el caso.** El investigador debe comprender los requisitos de las herramientas y tecnologías que se requieren para que el caso se investigue más a fondo.

Debe estar lo suficientemente cualificado y asegurarse de evitar que se sobrescriban los datos.

**PASO 03: Descubra y obtenga la evidencia:** el investigador debe asegurarse de no perder ninguna evidencia en la escena del crimen y obtenerla de la manera más precisa, que no cause ningún daño a la evidencia.

El investigador debe asegurarse de recolectar la muestra de evidencia en una bolsa de Faraday o en una bolsa antiestática para que la evidencia no pueda ser manipulada.

Debe asegurarse en todo momento de mantener la cadena de custodia.

**PASO 04: Haga múltiples copias forenses de la evidencia.** En la investigación forense digital, es muy esencial recordar que, en la medida de lo posible, nunca se debe trabajar con la evidencia original.

El investigador debe asegurarse de crear varias copias de las mismas y realizar un análisis de la copia de la evidencia original.

Antes de crear una copia de la evidencia, siempre debe calcular el valor hash de la evidencia recuperada en su forma original para mantener la autenticidad de la evidencia.

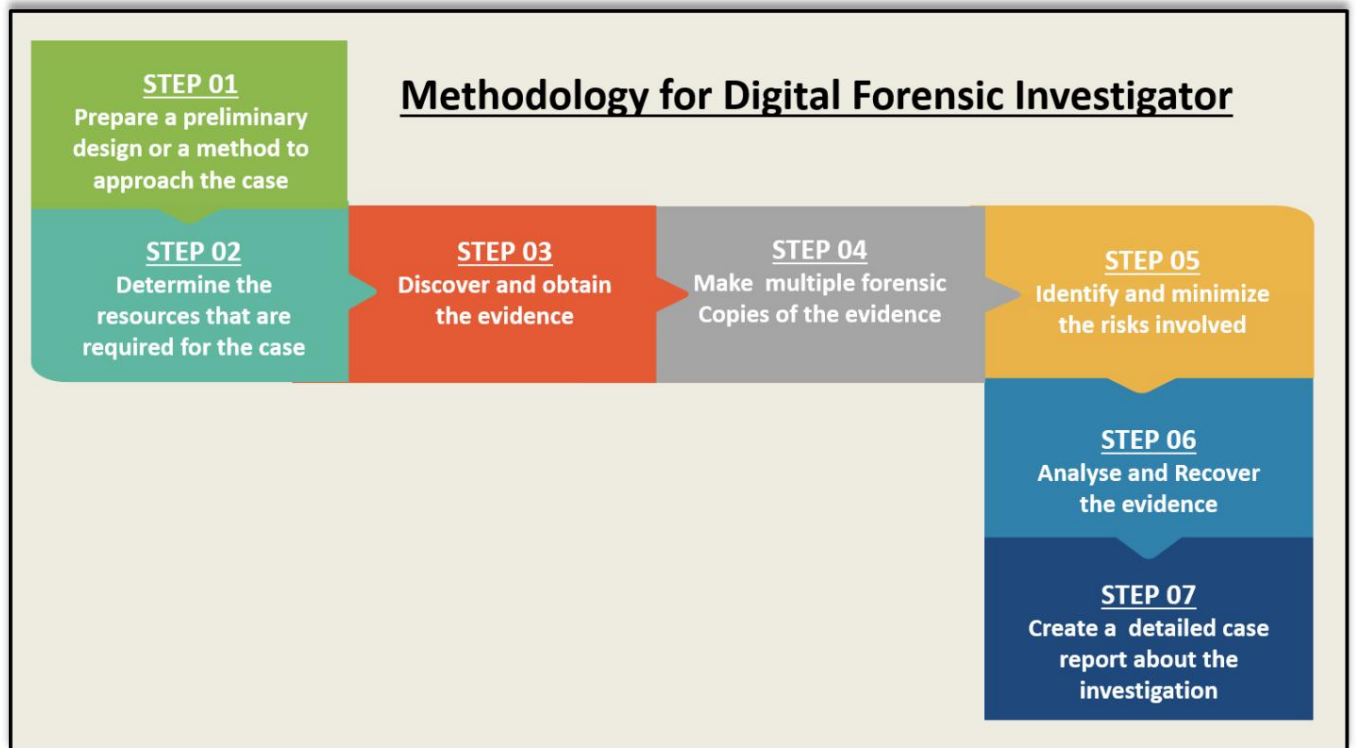
**PASO 05: Identificar y minimizar los riesgos involucrados.** El investigador debe recordar que la evidencia que se recopila no siempre es fácil de analizar. Hay una gran cantidad de riesgos y consecuencias involucradas. Debe estar lo suficientemente calificado para estimar la magnitud del riesgo y los posibles daños. Debería intentar encontrar mejores alternativas para minimizar el riesgo.

**PASO 06: Analizar y recuperar la evidencia:** una vez que el investigador tiene la evidencia, ahora puede comenzar a analizar la copia de la evidencia original utilizando varios programas comerciales y de código abierto que sean adecuados para ese caso. También puede utilizar varios programas para recuperar la evidencia que ha sido eliminado.

**PASO 07: Crear un informe de caso detallado sobre la investigación:** una vez que el investigador haya completado el análisis de la evidencia y haya encontrado artefactos importantes en la recuperación de datos, podrá crear un informe detallado sobre sus hallazgos, metodologías y herramientas utilizadas por él en la investigación.

Si lo requiere el jurado o el tribunal, el investigador debe representarse a sí mismo ante el tribunal como testigo experto para dar su testimonio sobre el caso en términos más simples para que las personas sin conocimientos técnicos comprendan mejor el caso.

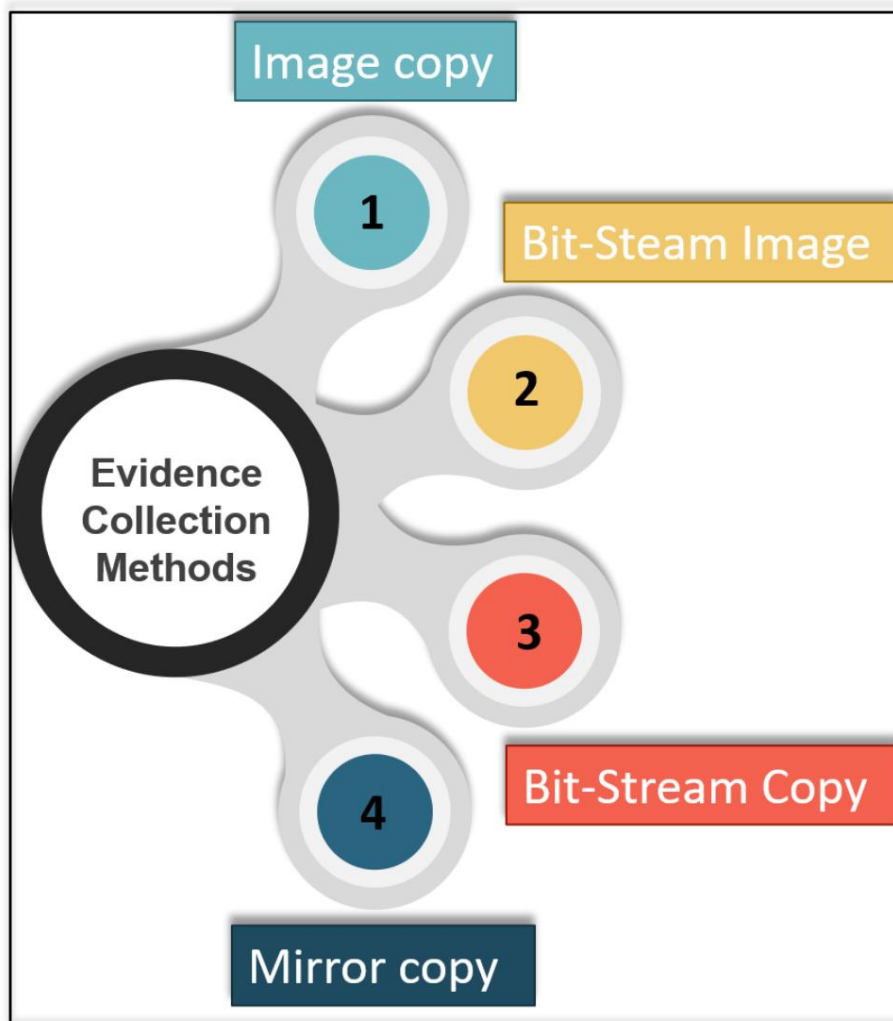




## Métodos de recopilación de pruebas

Los términos del método de recopilación de evidencia están interrelacionados y casi tienen el mismo propósito; lo único importante que debe recordar un investigador es que la copia debe ser sólida desde el punto de vista forense.

- **Copia de Imagen:** Se refiere a ser el duplicado del disco original.
- **Imagen Bit-Stream:** Es una copia clonada de la evidencia original. Incluye archivos de sectores, clústeres y recupera archivos eliminados de un disco.
- **Copia de flujo de bits:** una copia de flujo de bits se puede definir como una copia bit a bit de la evidencia original o del medio de almacenamiento, que puede ser su copia exacta. Una copia de flujo de bits también puede denominarse copia forense del disco.
- **Copia espejo:** una copia espejo es la réplica precisa (copia de seguridad) del disco.



# Imagen de disco y clonación

## Imágenes de disco

Es el proceso de realizar una copia de archivo o de respaldo de todo el disco duro. Es un archivo de almacenamiento que contiene toda la información necesaria para iniciar el sistema operativo. Sin embargo, este disco con imagen debe aplicarse al disco duro para funcionar. No se puede restaurar un disco duro colocando los archivos de imagen del disco en él, ya que es necesario abrirlo e instalarlo en el disco mediante un programa de imágenes. A

Un solo disco duro puede almacenar muchas imágenes de disco. Las imágenes de disco también se pueden almacenar en unidades flash de mayor capacidad.

## Clonación de discos

Es el proceso de copiar todo el contenido de un disco duro a otro, incluida toda la información que puede iniciar el sistema operativo desde el disco. Le permite crear una copia individual de uno de sus discos duros en otro disco duro. La otra copia del disco duro es completamente funcional y se puede intercambiar con el disco duro existente de la computadora. Si se inicia la unidad clonada, sus datos serán idénticos a los de la unidad de origen en el momento de su creación.

A continuación se muestra una diferencia simple entre imágenes de disco y clonación.

## DISK IMAGING & CLONING

### IMAGING

- Larger in size
- Compressed Copy
- Archival or a Backup Copy

### CLONING

- Comparatively Smaller in size
- Uncompressed Copy
- Replica of your Drive



## Desafíos que enfrenta el investigador del DF

**Cuestiones legales:** La cuestión más importante que puede encontrar un investigador es obtener la garantía de admisibilidad de la evidencia, lo que significa que debe ser aceptada por el tribunal.

**Naturaleza de la evidencia digital:** El avance de la tecnología ha impactado la investigación de tal manera que detectar la evidencia digital se ha vuelto extremadamente difícil. Por ejemplo, almacenamiento en la nube, PDA, dispositivos IoT, etc.

**Alteración de la evidencia:** La cadena de custodia debe mantenerse en todo momento para mantener intacta la credibilidad de la evidencia. Si la evidencia está en las manos equivocadas, la evidencia podría alterarse y perder su credibilidad. Por lo tanto, tener una imagen forense y el valor hash de la evidencia es extremadamente importante para el investigador.

**Tamaño y distribución de la evidencia:** El tamaño y la distribución de la evidencia son importantes porque los datos no son menores. Se produce una gran cantidad de datos con regularidad. En los casos de investigación forense de Big data, el tamaño y la amplia distribución de los datos suponen un desafío para el investigador, ya que no sabe por dónde empezar.

**Malware presente en la evidencia:** los delincuentes pueden ser más astutos que los investigadores e insertar malware en el dispositivo de evidencia que puede engañar o interrumpir la investigación en curso.

**Esteganografía:** en épocas anteriores, la esteganografía solo tenía tipos limitados, pero hoy en día, debido a la disponibilidad de diversas herramientas y software en la web oscura, se ha vuelto extremadamente difícil detectar la esteganografía presente en los elementos de evidencia. A veces, el investigador no lo considera como prueba porque no puede obtener muchas ideas detalladas sobre la evidencia.

**Cifrado:** Muchas veces, la evidencia se recupera en forma cifrada y el investigador tiene dificultades para descifrarla sin ninguna garantía de recuperación del contenido original.

### Challenges In Digital Forensic Investigation

Legal Issues

Nature of Digital Evidence

Alteration of Evidence

Size and Distribution of evidence

Malwares present in evidence

Steganography

Encryption

## Ventajas de la ciencia forense digital



• Su finalidad es asegurar la integridad del sistema digital.
• También ayuda a proteger el valioso dinero de la organización.
• Beneficia a las organizaciones registrar información esencial información en los casos en que los sistemas hayan sido comprometidos.
• Si la investigación se realiza eficientemente, ayuda a arrestar a los ciberdelincuentes a nivel mundial.
• Ayuda a producir pruebas correctas, que pueden ayudar a castigar al culpable.

## Contras de la ciencia forense digital



• Se debe demostrar que las pruebas digitales aceptadas ante el tribunal no han sido manipuladas.
• Almacenar y producir documentos electrónicos es caro
• Los profesionales del derecho carecen de conocimientos técnicos.
• La evidencia debe ser convincente y auténtica.
• Es posible que el tribunal no acepte herramientas de investigación no reconocidas

## Conclusión

Por lo tanto, en este artículo hemos cubierto los temas básicos que se requieren para tener una mejor comprensión de la Ciencia Forense Digital para otro nivel.

### Referencias

- <https://www.hackingarticles.in/digital-forensics-an-introduction/>
- <https://www.hackingarticles.in/digital-forensics-an-introduction-part-2/>



# ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

