# INFORMATICA FORENSE

**Siler Amador Donado**

**(Esp) Ingeniero de sistemas**

**Popayán-Colombia**

**samador@unicauca.edu.co**

- **Quien en un momento dado puede convertirse en un investigador de computación forense?...**

- **Que harían si su jefe les dice que hay un empleado al que creen que está vendiendo información a la competencia, y hay evidencias de eso en su computador ?...**

- **Que herramientas de trabajo se les ocurriría llevar a una investigación de computación forense ?...**

- **Que pasos llevarían a cabo en la investigación?**

# Contenido de la charla:

- **La ley 1273**
- **Qué es informática forense?**
- **Pasos en el proceso de computación forense**
- **Metodología de análisis de datos**
- **Cuales son las funciones de un investigador de computación forense?**
- **Eventuales interrogantes / inconvenientes en un operativo**
- **Herramientas de software**

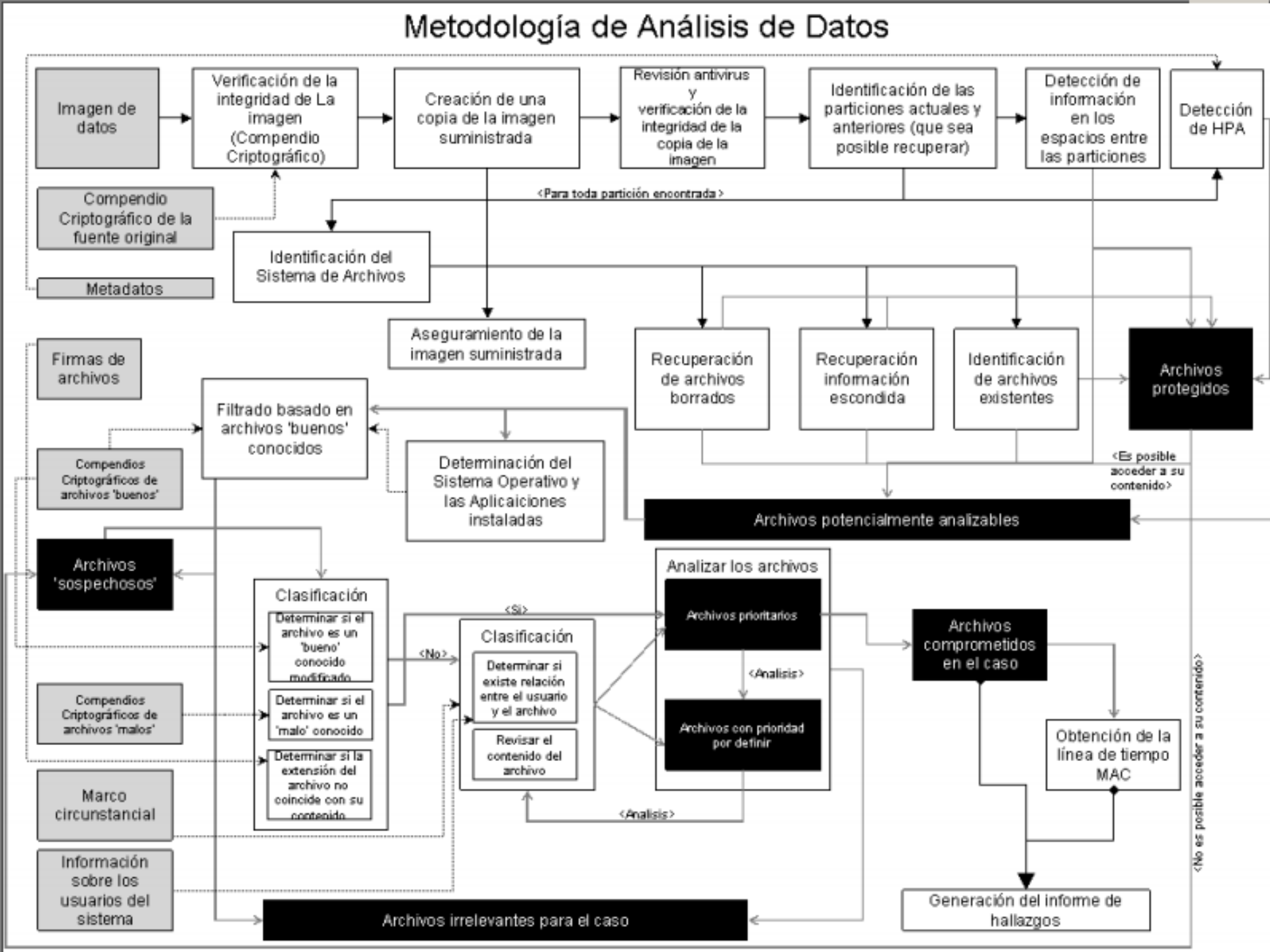
# QUÉ ES INFORMATICA FORENSE?

- La informática forense, también llamado cómputo forense, computación forense, análisis forense digital o examinación forense digital *es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal*. Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

# Pasos en el proceso de computación forense

- **Orden judicial o equivalente según la entidad**
- **Captura de la información en las instalaciones de los investigados (imágenes “forenses”)**
- **Análisis de la información capturada**
  - ✓ **Eliminación de información no útil**
  - ✓ **Búsquedas de acuerdo a parámetros relevantes de cada investigación**
- **Generación de reportes**
- **Entrega de información / evidencias encontradas**

# Metodología de Análisis de Datos



# Captura de información en un operativo:

- **Llevar una CPU rápida con varios DDs “probados”**
- **Solicitar acompañamiento del personal de soporte informático del investigado**
- **Determinar equipos a trabajar ( a capturar )**
- **Apagar equipos del investigado**
- **Retirar discos duros del investigado**
- **Instalarlos en la CPU rápida del “investigador en computación forense”, para realizar una “imagen forense”**
- **Instalar los DDs en sus equipos de origen y realizar una prueba con testigos**
- **Llevar imágenes al “laboratorio de computación forense” para el análisis**

# Funciones del investigador en Computación Forense

- **Capturar información en operativos de registro ( allanamientos)**
- **Protejer la integridad de la evidencia electrónica original**
- **Analizar las evidencias para encontrar pruebas que lleven a conclusiones**
- **Realizar informe / reporte de evidencias encontradas y pasarlo al jefe de la investigación**
- **Autenticar cualquier evidencia física originada de una fuente electrónica**

- **Problemas que se pueden encontrar en un operativo:**

  - Que pasa si se daña algún componente de hardware del investigado?
  - Que pasa si por error se sobre-escribe el disco duro del investigado? ( peor pesadilla !!! )
  - Que pasa si el investigado tiene un S.O. que no manejo?
  - Si el investigado tiene discos duros SCSI?... si tiene portátiles?...
  - Que medios de almacenamiento son susceptibles de ser capturados o copiados? ( SD, USB Flash, Celulares, PDAs )
  - Que pasa si el disco duro del investigado tiene sectores defectuosos?
  - Si el investigado alega que la información fue modificada?
  - Si tiene archivos encriptados o con contraseña?
  - Si tienen archivos de datos propios de un sistema específico, por ejemplo en RMCobol ?

- **Herramientas de hardware:**
  - **Accesorios para operativos**
  - **Sistemas completos**

# Accesorios para operativos:

- **Adaptadores IDE, SATA, SCSI, Portátiles, SM, MMC, etc.**
- **Bloqueadores de escritura de discos duros**
- **Memoria Flash USB ( > 1 GB )**
- **Discos duros externos USB / Firewire**
- **Quemador de DVD externo, con sus DVDs en blanco**
- **Cables “laplink”**
- **Cámaras digitales**
- **Herramientas: destornilladores**
- **Bolsas anti-estática para transportar discos duros**
- **Software de captura de “imágenes forenses”**

# Soluciones de Software en Computación Forense

# • Funcionalidades de un software de computación forense ( 1/ 2 )

- **Capturar la información de forma “forense”. ( Generalmente imágenes “forenses”)**
- **Compatibilidad con diferentes sistemas operativos**
- **Desplegar la información capturada de manera amigable, independientemente del sistema operativo, aplicativos y/o contraseñas ( visores )**
- **Impedir la modificación de cualquier atributo de la información capturada ( Preservación de evidencias )**
- **Registrar todas las actividades realizadas sobre las evidencias ( Logs de actividades realizadas )**
- **Generar scripts para automatizar procedimientos**

# • Funcionalidades de un software de computación forense ( 2 / 2 )

- **Poderosas opciones de análisis de la información: filtrar, explorar registro para determinar hardware, analizar “links”, idiomas, archivos cifrados, archivos comprimidos, ordenamientos, selecciones, análisis de uso en el tiempo de archivos, Outlook & Navegadores, entre otros.**
- **Eliminar archivos no relevantes a las investigaciones**
- **Hashing para eliminación o selección de información oculta**
- **Recuperar archivos eliminados por el usuario**
- **Realizar búsquedas de acuerdo a palabras clave**
- **Documentación y generación de reportes de los resultados encontrados**

- **Ejemplos de Software de Computación Forense:**

  - Encase
  - Digital Intelligence Forensic Toolkit
  - lLook
  - SMART ( Linux )

# Software: Encase

- Diferentes sistemas operativos ***
- Utilidad de captura de información ( imágenes ) ***
- Facilidad de visualización / navegación ***
- Preservación de evidencias ***
- Opciones de análisis ***
- Opciones de búsquedas ***
- Interpretación de Emails y actividad de Internet * * *
- Funcionalidades extendidas ***
- Generación de informes ***

# Software: ILook

- Quienes lo pueden usar ?
- Que agencias lo respaldan ?

# Fortalezas

- Completo
- En constante actualización
- Comunidad de investigadores mundial
- Gratis para agencias estatales

- **Consejos prácticos ( 1 / 2 )**

  - **Llevar discos duros externos con USB / FireWire, para evitar abrir computadores del investigado**
  - **Llevar discos duros en “exceso”, y ya probados**
  - **Tener números celulares de conocidos “expertos” en diferentes tipos de tecnologías**
  - **Realizar pruebas periódicas de los medios de almacenamiento que se lleven a los operativos**
  - **Sacar copias de la información capturada y trabajar sobre las copias**
  - **Llevar un quemador & CDs en blanco**
  - **Si es posible que haya testigos de la empresa / individuo investigado en el proceso de captura de la información, y realizar una prueba posterior**

- **Consejos prácticos ( 2 / 2 )**

  - **Bloquear los medios de almacenamiento del investigado contra escritura**
  - **Desconectar cables de red / modems, o apagar computadores**
  - **Anotar configuraciones de cables, jumpers, bahías, etc., antes de desconectar partes**
  - **Nunca “desfragmentar” un DD antes de capturar imagen, ni realizar otro tipo de utilidades**
  - **Tener mucha comunicación con los demás investigadores para obtener información relevante para búsquedas**
  - **Conocer a mayor profundidad el área donde se investigarán a los sospechosos. Ejm: IRS, DIAN**

- **Es fácil esconder / desaparecer evidencias de delitos en un computador ? …**

- **Está el estado colombiano en capacidad para encontrar evidencias digitales de actividades delictivas?....**

- **Vale la pena arriesgarse?...**

# MUCHAS GRACIAS …