



Curso de  
**Informática  
Forense**

---

Juan Pablo Caro

## Introducción

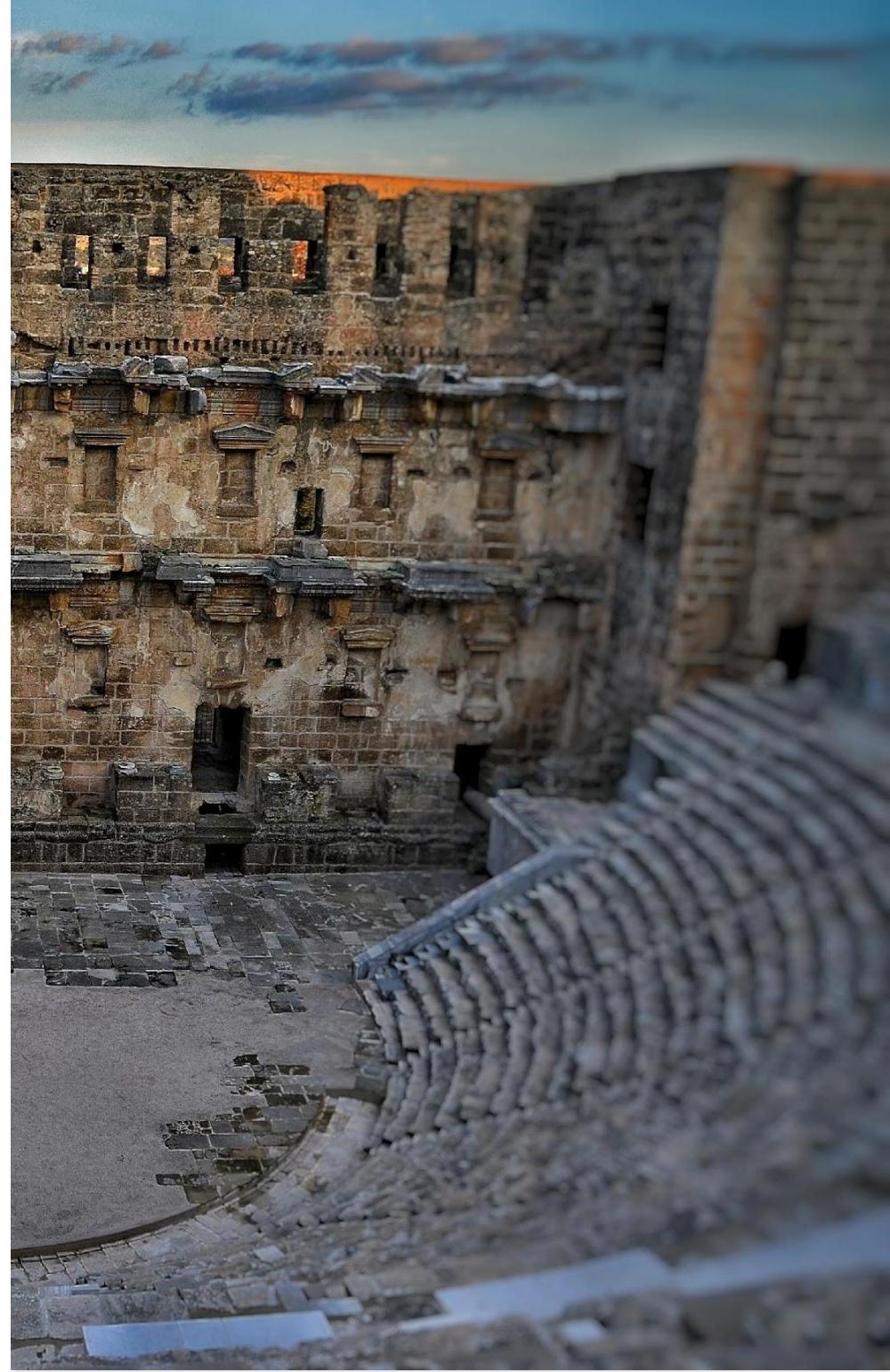
---

¿Qué es el cómputo forense?

---

# Ciencia Forense

Introducción general a  
la criminalística



---

# Ciencia forense

“**Forense**” del latín *forensis*: “delante del foro” / “frente al foro”.

“**Evidencia**” del latín *evidentia*: “visible”, “fácil de ver para cualquiera”.

## **Forense**

Que será presentado ante una corte o autoridad.

## **Evidencia**

Es visible para cualquiera.  
Debe poderse explicar fácilmente.

“

# La aplicación de la ciencia en un contexto legal.

”

*Richard Saferstein, “Criminalistics:  
An Introduction to Forensic Science”*

---

# Ciencia forense

La aplicación del método científico para establecer respuestas respecto a ciertos hechos en un contexto legal.

---

# 6 preguntas del proceso investigativo



¿Qué?



¿Dónde?



¿Cómo?



¿Quién?



¿Cuándo?



¿Por qué?

“Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto”

**Principio de Intercambio de Locard**

# Etapa I: Identificación



---

# Cómputo Forense

“Es el uso de métodos y técnicas científicas probadas, con el fin de identificar, preservar, validar, analizar, interpretar, documentar y presentar evidencia digital obtenida a partir de fuentes de información digital, con el propósito de facilitar la reconstrucción de hechos en una investigación legal, o ayudar a anticipar o prevenir acciones en contra de la ley.”

---

# Evidencia Digital

“Cualquier conjunto de datos almacenados de manera digital y que contengan información que pueda soportar o refutar una hipótesis de un incidente o acción criminal”.

---

# **Etapas del Cómputo Forense**

**Etapa I**



**Identificación**

**Etapa II**



**Preservación**

---

# **Etapas del Cómputo Forense**

**Etapa I**



Análisis

**Etapa II**



Presentación

Introducción

---

# Etapas I y II: Identificación y Preservación

---

# Identificación

Detectar, reconocer y determinar las fuentes de información que deben ser preservadas para una investigación.



## **6 Preguntas**

¿Cómo aplicar las 6 preguntas del proceso investigativo?

## **Preparación de herramientas**

Un kit de herramientas adecuadas para hacer adquisiciones.

## **Primer respondiente**

¿Quién es y qué debe hacer?

## **Toma de decisiones**

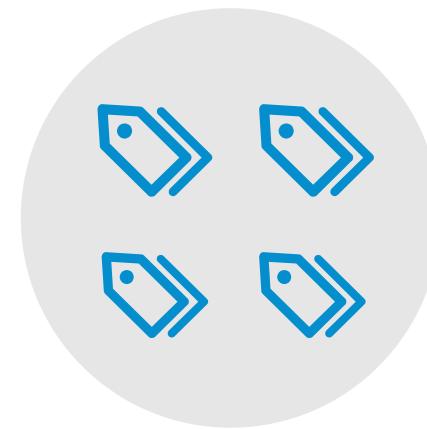
Adquisiciones “en vivo”, “estáticas”.

---

# Resultados de la Etapa I



Cadena de  
Custodia



Inventario de  
Fuentes

---

# **Etapa II: Preservación**



---

# Preservación

Recolección de información de dispositivos de almacenamiento de datos, para generar copias exactas usando técnicas forenses.



## **Medios de almacenamiento**

¿Qué son?, ¿Cuáles usamos comúnmente?, ¿Cómo funcionan?

## **¿Qué es una imagen forense?**

Definición, ejemplos y uso común.

## **Adquisición de imágenes forenses**

FTK Imager, Paladin Forensics, EnCase Imager, entre otras técnicas.

## **Algoritmos Hash**

¿Qué son y por qué los utilizamos?

---

# Resultados de la Etapa II



Imágenes  
forenses



Reportes de  
adquisición y  
verificación

Introducción

---

# Etapas III y IV: Análisis y Presentación

---

# Etapa III: Análisis



---

# Análisis

Procesamiento de información relacionada con el objetivo de la investigación, con el fin de determinar hechos asociados con un evento.



---

# Análisis

- Análisis Preliminar
- Análisis de Sistemas Windows
- Análisis de Sistemas Unix



## **Sistemas de Archivos**

¿Qué son?, ¿Cuáles usamos comúnmente?, ¿Cómo funcionan?

## **Creación de imágenes parciales**

Clasificación de datos para análisis

## **Exportado de archivos**

Separación de información

## **Análisis preliminar de Sistemas Operativos**

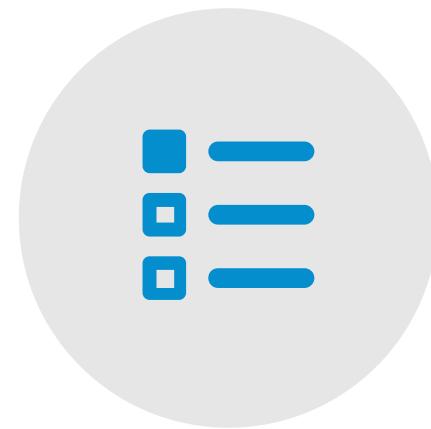
Windows y Unix

---

# Resultados del Análisis Preliminar



Información  
filtrada para  
análisis



Reporte  
preliminar de  
análisis



**Análisis de usuarios de sistema**  
¿Qué usuarios han estado activos  
en el sistema?

**Análisis de logs y procesos ejecutados**  
Reconstrucción de la actividad del  
Sistema Operativo

**Recuperación de archivos borrados**  
Reconstrucción y procesos de data  
carving

**Artefactos específicos de Sistema**  
Diferencias entre Windows y Unix

---

# Resultados del Análisis General



Resultados generales de la investigación



Posibles fuentes adicionales de consulta

---

# **Etapa IV: Presentación**



# Presentación

Entrega de resultados,  
con un lenguaje adecuado,  
en forma de reportes  
a las partes interesadas  
o autoridades que los  
requieran.





**Organización de la información**  
¿Qué debemos incluir y qué no?,  
¿Cómo presentar los resultados y qué decir?

**Creación de un informe técnico**  
¿Qué detalles debemos incluir?

**Creación de un informe ejecutivo**  
¿Qué lenguaje debemos utilizar?,  
¿Cómo resumir nuestros hallazgos?

**Presentación ante autoridades**  
Consejos y recomendaciones

---

# Resultados de la Presentación



Informe Técnico



Informe  
Ejecutivo

Etapa I: Identificación

---

# Preparación de un kit para adquisición

---

# Kit de adquisición

## Hardware

- Laptop (Windows / Linux)
- Protectores contra escritura
- Cámara digital
- Discos duros externos

## Herramientas

- Kit de destornilladores
- Cables de red
- Cables SATA e IDE
- Pinzas
- Linternas
- Precintos para cables

## Software

- Linux Live USB: (Paladin Forensics / Kali / Otra )
- EnCase Imager
- FTK Imager Lite

---

# Kit de adquisición

## Papelería

- Documentos y formatos impresos
- Grapadora
- Notas de colores y banderitas
- Cinta de enmascarar
- Marcadores, bolígrafos, lápices
- Tijeras

## Otros

- Bolsas anti-estática
- Precintos (velcro / plástico)
- Bolsas de evidencia
- Baterías
- Almacenamiento externo
- Multitoma
- Hub USB
- Cargadores y cables extra

Etapa I: Identificación

---

# Proceso de Cadena de Custodia

---

# Cadena de Custodia



---

# Cadena de Custodia

Procedimiento documental en el cual se registra la responsabilidad y custodia de los elementos de evidencia digital, desde su adquisición o generación, hasta su disposición final.

## **Seguimiento documental**

Usando un formato más o menos estándar, se hace seguimiento a la evidencia.

## **¿Quién tiene la evidencia y cuándo?**

El proceso y la documentación ayudan a saber quién es el responsable de la evidencia en cada momento.

## **Soporte legal para el proceso de investigación**

La CoC (Chain of Custody) es un proceso estándar aceptado a nivel internacional.

Etapa I: Identificación

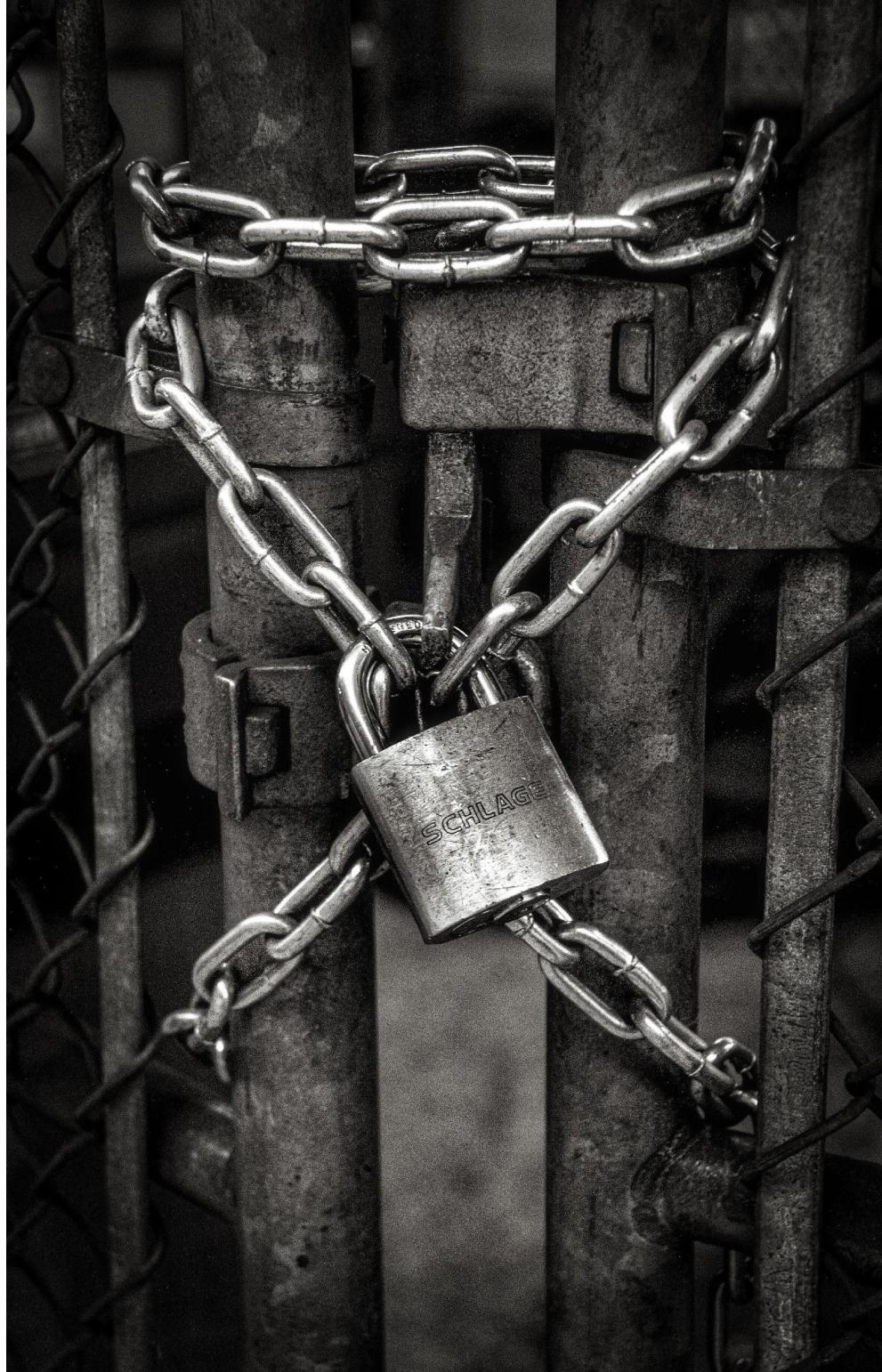
---

# Inventario de Evidencia

---

# Primer respondiente

- ¿Quién es?
- ¿Cómo debe estar preparado?
- ¿Qué alcance tiene?







## Adquisición estática

Sistemas que están apagados o que no se modifican o alteran al apagarse.



## Adquisición en vivo

Sistemas que no pueden apagarse, o que al apagarse pierden información relevante.

---

# Inventario de Evidencia

- Número Identificador
- Custodio
- Tipo de dispositivo
- Marca
- Modelo
- Número de Serie
- Número de Inventario
- Capacidad de Almacenamiento
- Notas

# Inventario de Evidencia

Etapa II: Preservación

---

# Creación de una imagen forense

---

# Imagen Forense

Copia “bit-a-bit” exacta del contenido de un medio de almacenamiento, que utiliza algún método de verificación digital para garantizar la autenticidad de la información.

