
SEGURIDAD
CERO
CURSO GRATIS
INVESTIGACIÓN Y
CÓMPUTO FORENSE

SEGURIDAD CERO

PROGRAMA COMPLETO

INVESTIGACIÓN Y CÓMPUTO FORENSE

~~600 USD~~ 239USD

Presiona aquí

SEGURIDAD CERO

CLASE #3

Investigación Forense

MIERCOLES 25 NOVIEMBRE

CRI	GTM	HND	MEX	PER
6:00 PM	6:00 PM	6:00 PM	6:00 PM	7:00 PM

COL	ECU	PAN	PRY	CHL
7:00 PM	7:00 PM	7:00 PM	8:00 PM	9:00 PM

BOL	VEN	DOM	ARG	URY
8:00 PM	8:00 PM	8:00 PM	9:00 PM	9:00 PM

SEGURIDAD CERO

Fernando Conislla

Cybersecurity Expert

- Años de experiencia en servicios de ciberseguridad para entidades gubernamentales, bancarias, medios de pago, etc.
- Instructor SEGURIDAD CERO e instructor oficial ISO 27001
- Expositor en eventos internacionales
- Master en gestión y dirección de la ciberseguridad
- Certificaciones internacionales CEH, ISO 27001 LA, LCSPC.

SEGURIDAD CERO

Ingrid Santisteban

Computer Forensic Investigator

- Experta en la investigación de delitos informáticos, forense digital, auditoria y riesgos de TI.
- Instructor en SEGURIDAD CERO
- Maestría en Informática Forense y Seguridad de la Información
- Certificada internacionalmente como Investigador Digital Forense (IDF)

Introducción al Análisis Forense

El concepto de análisis forense digital hace referencia a un conjunto de procedimientos de recopilación y análisis de evidencias que se realizan con el fin de responder a un incidente relacionado con la seguridad informática y que, en ocasiones, deben de servir como pruebas ante un tribunal. Mediante este procedimiento se pretende responder a las siguientes preguntas: *¿qué?, ¿dónde?, ¿cuándo?, ¿por qué?, ¿quién? y ¿cómo?*

FASES DEL ANÁLISIS FORENSE

Preservación	Corresponde a la fase en la que se debe garantizar que no se pierdan las evidencias que deben ser recopiladas para su posterior análisis
Adquisición	Corresponde a la fase en la que se recopilan las evidencias
Análisis	Es el examen de la evidencia recopilada.
Documentación	Documentar todos y cada uno de los pasos realizados durante el proceso
Presentación	Explicar de manera clara el proceso que se ha llevado para la obtención de las evidencias.

TIPOS DE ANÁLISIS FORENSE DIGITAL

Se puede crear una clasificación de tipos de análisis forense digital en base al área específica dentro de las tecnologías de información hacia donde se encuentre orientada.

Teniendo en cuenta este aspecto se pueden identificar tres tipos de análisis:

- Análisis forense de sistemas: tanto sistemas operativos Windows, como OSX, GNU/Linux, etc.
- Análisis forense de redes y telecomunicaciones.
- Análisis forense de dispositivos móviles
- Análisis forense de memoria volátil.

DISPOSICIONES ESPECIALES

Para preservar la evidencia volátil de un ordenador o computador se deben evitar las siguientes acciones con el fin de no invalidar el proceso de recolección de información ya que debe preservarse su integridad con el fin de que los resultados obtenidos puedan ser utilizados en un juicio en caso de ser necesario.

- No apagar el ordenador hasta que se haya recopilado toda la información volátil
- No confiar en la información proporcionada por los programa del sistema ya que pueden haberse visto comprometidos, se debe recopilar la información mediante programas desde un medio protegido como se explicará más adelante.
- No ejecutar programas que modifiquen la fecha y hora de acceso de todos los ficheros del sistema.

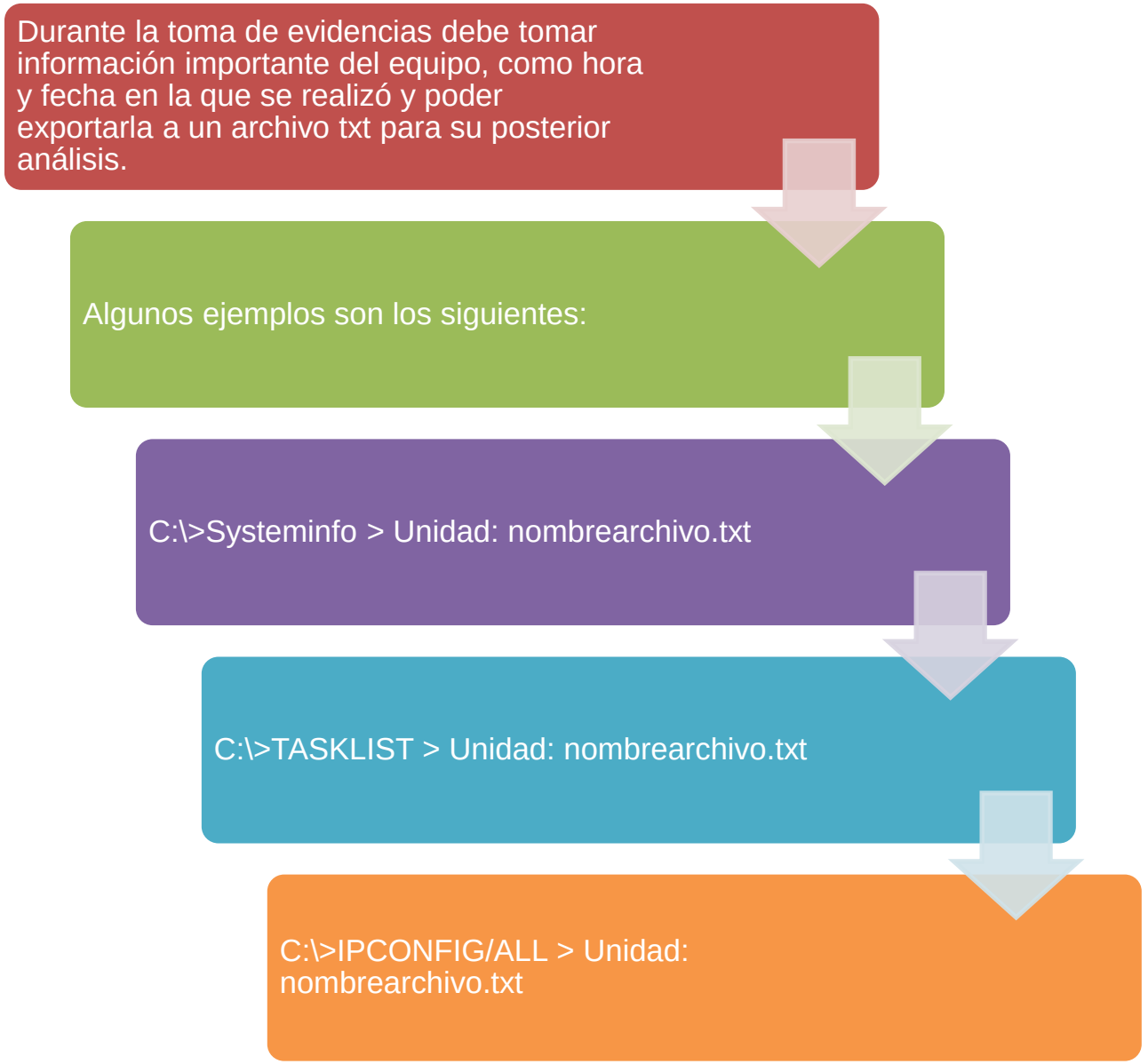
IDENTIFICACIÓN DE INDICIOS EN LA ESCENA

OBTENSIÓN DE INFORMACIÓN DE EQUIPO DE CÓMPUTO

- Un aspecto muy importante al estar frente a un equipo de cómputo encendido y desbloqueado que puede ser objeto de investigación de un hecho delictivo, es tomar primero las evidencias volátiles y después las que no lo son, en este sentido, se suele realizar únicamente un volcado de memoria o de el disco duro, y a partir de ellas trabajar sobre diferentes copias para obtener el resto de las evidencias.

- A continuación se ejemplifican algunos comandos que pueden ser útiles al momento de tomar evidencia concreta de un equipo.

Algunos comandos útiles en la toma de evidencia



SEGURIDAD CERO

CLASE #3

Investigación Forense

MIERCOLES 25 NOVIEMBRE

CRI	GTM	HND	MEX	PER
6:00 PM	6:00 PM	6:00 PM	6:00 PM	7:00 PM

COL	ECU	PAN	PRY	CHL
7:00 PM	7:00 PM	7:00 PM	8:00 PM	9:00 PM

BOL	VEN	DOM	ARG	URY
8:00 PM	8:00 PM	8:00 PM	9:00 PM	9:00 PM

SEGURIDAD CERO

PROGRAMA COMPLETO

INVESTIGACIÓN Y CÓMPUTO FORENSE

~~600 USD~~ 239USD

Presiona aquí


SEGURIDAD
CERO
CURSO GRATIS
INVESTIGACIÓN Y
CÓMPUTO FORENSE