



TEMARIO DE CÓMPUTO FORENSE

PROGRAMA DE TECNOLOGÍA EN CÓMPUTO

ENERO 2016

1. Introducción a la informática forense

- a. ¿Que es la informática forense?
- b. ¿Cuándo podemos aplicar la ciencia de informática forense?
- c. Escena del crimen
- d. Evidencias
- e. Equipo mínimo de trabajo
- f. Informática y crimen
- g. Secuencia de análisis forense
- h. Paralelismo con la ciencia forense tradicional

2. Escena del crimen digital

- a. Sistemas basados en UNIX
- b. Sistemas basados en Windows

3. Cadena de custodia

- a. Procedimiento
- b. Responsables

4. Evidencias

- a. Evidencia forense lógica
- b. Evidencia forense bit a bit
- c. Preservación, Observación, fijación, levantamiento, etiquetamiento, traslado al laboratorio
- d. Interpretación de evidencias

5. Entorno informático y criminales

- a. Grupos de cibernaciones
- b. Perfil de los cibercriminales
- c. Alcances de la informática forense

6. Sistemas de archivos

- a. Organización de los datos
- b. Particiones de disco
- c. Capas de sistemas de archivos
- d. Análisis del MBR





TEMARIO DE CÓMPUTO FORENSE

PROGRAMA DE TECNOLOGÍA EN CÓMPUTO

ENERO 2016

- e. Datos alojados o sin alojar
- f. Capas de metadatos
- g. Apuntadores e inodos
- h. Sistemas de archivo ext2/3, NTFS y FAT32/16
- i. Entradas MFT
- j. Recolección manejo y análisis de la evidencia

7. Análisis forense sobre entornos windows

- a. Etapas del análisis
- b. Análisis externo
- c. Análisis de tráfico

8. Uso de FTK, OSForensics, Helix y Autopsy

- a. Generación de copias bit a bit
- b. Montaje de imágenes
- c. Análisis de registros

9. Evidencia digital

- a. Evidencia digital
- b. Memoria volátil
- c. Metodologías y herramientas para generar imágenes de disco
- d. Autentificación de la preservación de la evidencia
- e. Reconocimiento del tipo de evidencia
- f. Análisis de imágenes de disco y de RAM

10. Entornos virtuales

- a. Máquinas virtuales
- b. Virtualización de entornos informáticos
- c. Uso de software para virtualización

11. Gestión, control, tratamiento y manejo de la evidencia

- a. Recuperación de contraseñas
- b. Flujos alternos de datos
- c. Analizadores de archivos
- d. Documentos encriptados





TEMARIO DE CÓMPUTO FORENSE

PROGRAMA DE TECNOLOGÍA EN CÓMPUTO

ENERO 2016

- e. Criptografía
- f. Esteganografía

12. Análisis forense sobre dispositivos móviles Android

- a. Análisis forense a dispositivos Android
- b. Sistema de archivos y arquitectura
- c. Configurando el laboratorio forense y los emuladores
- d. Acceso a la información de los dispositivos
- e. Adquiriendo la evidencia digital
- f. Análisis de la evidencia adquirida
- g. Analisis de Contactos, Llamadas, Mail, Fotos y Videos, Mensajes de Texto
- h. Calendario y demás información almacenada en el dispositivo
- i. Análisis Con Herramientas libres y comerciales

