



Curso IF02

INFORMATICA FORENSE : ANALISIS DE EVIDENCIA DIGITAL

1. **Descripción** : Es un curso orientado a profesionales informáticos , investigadores forenses con interes en conocer diversos procedimientos de Análisis forense de sistemas informáticos , tanto del sector privado como del público incluyendo fuerzas de la ley.
2. **Alcance** : Delitos en tecnología . Análisis de evidencia Informática . Investigación corporativa. Investigación local y análisis forense en redes .
3. **Duración** : El curso consta de 2 clases teórico prácticas de 4 horas cada una dictada con frecuencia semanal o bi semanal.
4. **Prerequisitos** : Se requiere Conocimientos de evidencia informática (Equivalentes al curso IF01) . conocimientos de Windows 9x/2000/NT/XP y de protocolo TCP/IP (numeracion , DNS , DHCP).
5. **Dinámica de las clases** : Exposición oral con presentación de powerpoint reforzada con el uso del pizarrón. Se presentarán numerosas aplicaciones forenses comerciales y de uso libre. Se harán demostraciones “en vivo”.
6. **Contenido de las clases** :
 - **Clase 1**: Estructúra de *file system* en windows : FAT/FAT32/NTFS. Validación de datos. Búsqueda datos en la estructúra en bruto de un



disco . Identificadores de archivo y contenido del mismo. Búsqueda de datos en espacio no asignado y en espacio descuidado (slack space). Utilización de aplicaciones comerciales para realizar búsquedas en menor tiempo. Principios de recuperación de datos. Búsquedas complejas de datos empleando sintáxis GREP.

- **Clase 2:** Análisis de firmas e índices de archivos. Análisis de registro de windows. Investigación de medios removibles. Investigación del spool de impresión. Clientes de correo electrónico. Archivos LNK . Análisis forense de sesiones CD/DVD. Análisis y adquisición “en vivo” . Demostración con ejemplos de casos reales