



Curso IF01

INFORMATICA FORENSE

ADQUISICION DE EVIDENCIA DIGITAL

1. **Descripción** : Es un curso orientado a profesionales informáticos , de auditoría y profesionales de otras especialidades con conocimientos informáticos y con interés en conocer las reglas de buena práctica y los procedimientos de adquisición forense de sistemas informáticos , tanto del sector privado como del público incluyendo fuerzas de la ley.
2. **Alcance** : Delitos en tecnología . Evidencia informática . El rol del investigador forense informático. Actividad judicial y extrajudicial . 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 a determinar . Adicionalmente se pueden incluir otras 4 horas de laboratorios demostrativos de adquisición de evidencia digital con herramientas libres y versiones de evaluación.
4. **Prerequisitos** : Se requiere conocimientos de sistemas operativos Windows y Linux.
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** : Informatica forense : Definiciones .Obtención de Evidencia digital : Conductas a seguir por el experto forense en la “escena del crimen”. Captura de datos y monitoreo de comunicaciones . Análisis de sistemas independientes y de estaciones en red. Recolección de datos mediante imágenes de disco . Distintos formatos de adquisición forense.. Autenticación de evidencia digital mediante un algoritmo de hash. Adquisición directa e indirecta . Almacenamiento y transporte de evidencia digital.
- **Clase 2**: Adquisición de evidencia con software libre y con software propietario. Conversión entre distintos formatos. Uso del bloqueador de escritura de software y de hardware .
Demostración de adquisición en formato “dd” empleando el live CD forense Helix 3. Adquisición usando “Encase Forensic” y conversión de formatos con “FTK Imager” . Duplicación forense por hardware.
- **Clase 3**: Laboratorios demostrativos de obtención y preservación de evidencia con material que se entregará a los asistentes para su propia práctica .



7. **Docente:** Gustavo Daniel Presman : Ingeniero Electrónico egresado en 1987 de la Facultad de Ingeniería UBA . Posee las certificaciones Internacionales CCE (Certified Computer Examiner) , EnCE (Encase Certified Examiner) y ACE (Access Data Examiner). Cuenta con mas de veinte años de actividad profesional privada en las areas de Informática y redes de computadoras . Profesor titular del Instituto de tecnología ORT y de los posgrados en seguridad de la Información de la UBA y de la USAL y en Derecho Informatico de la UNSL. Perito Judicial en Informática y electrónica con actuación en la Suprema Corte de Justicia , Cámaras nacionales y de la provincia de Buenos Aires. Perito de las listas oficiales en Sistemas Computarizados del departamento judicial de San Isidro. Consultor en Investigación corporativa y entrenador de Fuerzas Armadas , Poderes judiciales provinciales y Policías de nuestro país en Investigación Forense Informática.