



Curso IF12

INFORMATICA FORENSE

ADQUISICION Y ANALISIS DE EVIDENCIA DIGITAL

1. **Descripción** : Es un curso orientado a profesionales informáticos y afines , de auditoría , y abogados 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 tiene una duracion de 20 hs. y puede ser dictado con frecuencia a determinar de común acuerdo.
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. **Metodología** : *in company*



7. 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. Marco regulatorio .Leyes vinculadas a TI. Ley de delitos informaticos (Ley 26388). Actuación profesional pericial y consultoría técnica de parte.
- **Clase 2** : 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 3**: 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 . Adquisición usando “Encase Forensic” y conversión de formatos con “FTK Imager” . Duplicación forense por hardware.
- **Clase 4**: 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. Análisis de firmas e índices de archivos. Análisis de registro de windows. Investigación de medios removibles. Investigación del spool de impresión

- **Clase 5:**. Analisis de actividad en Internet . Clientes de correo electrónico. Investigacion de correo electronico en servidores . Determinacion de emisores y analisis de sesiones de chat.Archivos LNK . Análisis forense de sesiones CD/DVD. Análisis de casos reales

8. **Docente:** Gustavo Daniel Presman : Ingeniero Electrónico egresado en 1987 de la Facultad de Ingeniería UBA . Posee las certificaciones Internacionales CCE (Certified Computer Examiner) y EnCE (Encase Certified Examiner) . Cuenta con 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 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.