



Curso / Taller IF03

PROCESAMIENTO FORENSE INFORMATICO

1. **Descripción** : Este taller es un laboratorio de Informática forense en el cual los asistentes resolverán , las distintas etapas del análisis forense Informático : Adquisición , Preservación , Análisis e Informe , sobre un caso ficticio que será puesto a disposición de los asistentes .

Se validarán adquisiciones de archivos de evidencia con la distribución forense Helix y posteriormente se procesaran algunas búsquedas utilizando software libre linux/Windows.

2. **Objetivos** :

- Reforzar conceptos de adquisicion de evidencia Informática
- Evaluar metodologías para procesar un caso mediante Informática forense.
- Ejecutar de procedimientos técnicos de Análisis forense Informático

3. **Duración** : El taller tiene una duración de 8 hs. en un día completo

4. **Nivel** : Intermedio /Avanzado

5. **Prerequisitos** : Los asistentes deberán poseer conocimientos de informática Forense y concurrir con sus notebooks para la realización de este taller (Configuración mínima : Windows XP Pro / 1 GB de RAM / 4 GB de espacio libre en HD/ 2 USB libres/ Unidad CD booteable)



6. **Infraestructura Necesaria** : Cañón para proyectar y pizarrón . Tener presente que será necesario espacio físico cómodo para los asistentes y sus notebooks (tomacorrientes de alimentación) .

No es necesario conexión a Internet ni Infraestructura de red.

8. **Entregables** : Los asistentes reciban material electrónico con las aplicaciones que se utilizarán durante el taller (software libre y versiones de evaluación) , así como también los archivos de evidencia necesarios.

8. **Desarrollo / Contenido** : Adquisición de evidencia con “dd” , Linen y FTK Imager . Interoperabilidad y conversión de formatos . Validación de la evidencia . Preprocesamiento de un caso : Verificación . Zona horaria . Análisis de estructura de file system en windows: FAT/FAT32/NTFS. Validación de datos. Búsqueda de datos en la estructura 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). Búsquedas complejas de datos empleando sintaxis GREP. Investigación del spool de impresión . Análisis forense de actividad en Internet ..

1. **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 más de veinte años de actividad profesional privada en las áreas 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.