

Informática Forense

Objetivo:

- Identificar y Caracterizar las etapas de un Peritaje Informático Forense, y la relación intrínseca entre éstas y el Marco Legal Vigente.
- Comprender exhaustivamente los Procedimientos técnicos a seguir en la Identificación / Adquisición, Preservación, Análisis y Presentación de la Evidencia Digital.
- Identificar y Seleccionar las Herramientas Forenses adecuadas para su utilización en cada etapa.
- Desarrollar habilidades básicas en el uso de las principales Herramientas Forenses.
- Correlacionar Casos Ejemplificadores con el uso de Herramientas Forenses en cada etapa.

Programa analítico de la capacitación:

UNIDAD 1: ASPECTOS PRELIMINARES.

- 1.1. Origen y Conceptos de las Ciencias Forenses.
- 1.2. Bases Doctrinarias y Técnicas. Cuándo, Dónde, Cómo, Qué, Quién, Por Qué
- 1.3. La Pericia Forense Informática : Conceptos universalmente aceptados.

UNIDAD 2: MARCO NORMATIVO LEGAL

- 2.1. Existencia Legal del Perito Informático y la Evidencia Probatoria.
- 2.2. Consideraciones de la Ley. Constitución Política de Bolivia. Modificaciones.
- 2.3. Leyes con reconocimiento de Documentos Electrónicos y Delitos Informáticos. Ley 1322, 1438, 1439, 1455, D.S. 24771 y D.S. 24582
- 2.4. El Código Penal. Reformas. Ley 1768/97. Capítulo XI.
- 2.5. Ley 1836 del Tribunal Constitucional
- 2.6. El Código de Procedimiento Penal. Ley 1970. Modificaciones. Decretos Legislativos 957 y 959.
- 2.7. Otras Leyes relevantes : Ley 1990, 2027, 2175, 2492, D.S. 23318-A
- 2.8. El Proyecto de Ley de Comunicación Electrónica y Comercio Electrónico : Aportes a la modernización del Código Penal, Civil y Procedimentales.
- 2.9. Doctrina Legal Internacional sobre las Condiciones Jurídicas de la Evidencia Digital.

UNIDAD 3: IDENTIFICACION Y ADQUISICION DE LA EVIDENCIA DIGITAL

- 3.1. Entendiendo la Evidencia Digital. Evidencia y Medios. Los tiempos en el proceso de Identificación.
- 3.2. Mutabilidad de la Evidencia Digital. Evidencia Perdurable y Volátil. Formas de Identificación.
- 3.3. Evidencia Perdurable : Identificación de Medios de Almacenamiento. Adquisición.
- 3.4. Evidencia Volátil : Identificación de la existencia. Monitoreos de Red. Formas de Adquisición.
- 3.5. Herramientas de uso común para la Identificación y Adquisición.
- 3.6. Casos Ejemplificadores. Ventajas e inconvenientes.

UNIDAD 4: PRESERVACION DE LA EVIDENCIA DIGITAL

- 4.1. Fragilidad de la Evidencia Digital. Escena del Crimen, Contaminación y Nulidad de la Prueba.
- 4.2. Procedimientos para la Preservación de la Evidencia con conformidad legal. Flujograma.
- 4.3. De la Escena del Crimen a la Cadena de Custodia. Apagado y Retiro de Evidencia Digital.
- 4.4. Documentación del Proceso. Uso del Reloj Patrón. Time Stamping
- 4.5. Validación de la Prueba preservada : Checksum y Hash.
- 4.6. Casos especiales de Preservación de Evidencia Volátil. Preparación de la Escena. Recolección. Memory Dumps. Sniffers y Monitores. Process List & Tracking.
- 4.7. Evidencia Remota. Crawlers. Adquisición por Web. Web Dumpers. Wget.
- 4.8. Herramientas para la Preservación de la Evidencia Digital.
- 4.9. Casos Ejemplificadores. Ventajas e inconvenientes.

UNIDAD 5: ANALISIS FORENSE DE LA EVIDENCIA DIGITAL

- 5.1. Requisitos Técnico-Legales para Analizar la Evidencia Digital.
- 5.2. Recreación Cronológica de hechos. Importancia de los Registros, la Documentación y el Uso del Reloj Patrón. Tiempo crítico de Cadena de Custodia en el almacenamiento de la Evidencia.
- 5.3. Preparación de Evidencia Analizable : Copias. Casos Especiales de Análisis Unico por Destrucción. Documentación del Proceso. Comprobación de identidad por Hashing o Checksums
- 5.4. Buceando en los Datos. Técnicas de Análisis. Revisión de Logs, Archivos Temporales, Swappings, Cachés, Recycleds, Spools y similares. Recuperación de Datos relevantes. Scaneo de los Medios por FileSystems o por Geometría Física.

5.5. Tipos comunes de datos : Mails, Imágenes, Documentos de Ofimática. Los Metadatos. Interpretación.

5.6. Dispositivos Móviles y Hands. Análisis por Revisión o Extracción.

5.7. Variedad de Herramientas para el Análisis Forense de la Evidencia Digital.

5.8. Casos Ejemplificadores. Ventajas e inconvenientes.

UNIDAD 6: PRESENTACION JUDICIAL DE LA EVIDENCIA DIGITAL

6.1. La Documentación del Análisis Forense como base para la elaboración del Informe Pericial. Informe

Unico y en Disidencia. Fundamentación Técnica.

6.2. Contenido de un Informe Pericial. Rubricado.

6.3. Ampliación del Informe por vía oral. Juicio Oral. Acompañamiento de Notas. Uso de Recursos Técnicos.

Los Consultores Técnicos en el Proceso del Interrogatorio. Delimitación Conceptual de las afirmaciones y conclusiones del Perito. Juicio de Valor. Uso de Lenguaje.

Audiencia:

Profesionales, Administradores y Responsables de Seguridad de la Información, Profesionales de Sistemas, Consultores de Tecnología y Auditores Internos y Externos de IT

Requisitos del Participante

- Conocimientos generales en Informática, Sistemas Operativos y Ofimática.
- Conocimientos generales en Criminalística, Escena del Crimen y Administración de Evidencia (Cadena de Custodia)
- Conocimientos avanzados sobre Procedimiento Civil y Penal y Garantías Constitucionales.
- Conocimientos generales sobre Legislación en áreas específicas tales como : Delitos Informáticos, Telecomunicaciones, Función Pública, Privacidad y Propiedad Intelectual

Duración:

16 hs.

Materiales a Entregar:

Carpeta y CD con las presentaciones y herramientas utilizadas durante la capacitación.