

Identificación y Adquisición de Evidencia Digital

Objetivo:

- Identificar y Adquirir Evidencia Digital en las diferentes etapas de un Proceso Judicial.
- Comprender exhaustivamente los Procedimientos técnicos a seguir en la Identificación y Adquisición de la Evidencia Digital.
- Manejar adecuadamente la Adquisición de Evidencia Digital en la Escena del Crimen.
- Utilizar los recursos técnico-legales apropiados para la Adquisición de Evidencia Digital fuera de la Escena del Crimen.
- Desarrollar habilidades básicas en el uso de las principales Herramientas Forenses.
- Correlacionar Casos Ejemplificadores con el uso de Herramientas Forenses.

I. PROGRAMA ANALITICO DE LA CAPACITACION.

UNIDAD 1: ASPECTOS PRELIMINARES.

- 1.1. Entendiendo la Evidencia Digital. Evidencia y Medios. Los tiempos en el proceso de Identificación.
- 1.2. Mutabilidad de la Evidencia Digital. Evidencia Perdurable y Volátil.
- 1.3. Formas de Identificación de la Evidencia Digital.
- 1.4. Caminando sobre la Evidencia.

UNIDAD 2: EVIDENCIA DIGITAL PERDURABLE

- 2.1. Los Medios de Almacenamiento. Heterogeneidad y miniaturización.
- 2.2. Concepto amplio de Perdurabilidad. Las memorias Flash. Las tarjetas.
- 2.3. Dispositivos de Seguridad : Firewalls, IDS, IPS.

UNIDAD 3: EVIDENCIA DIGITAL VOLATIL

- 3.1. Evidencia Volátil : Identificación de la existencia.
- 3.2. Las Memorias. Tipos de Memorias. Tiempos de borrado.
- 3.3. Monitoreos de Red. Formas de Adquisición.
- 3.4. Herramientas de Hacking para la Inspección, Identificación y Adquisición de Evidencia Digital. Uso Legal y uso espurio.
- 3.5. Captura de Evidencia Digital por Interceptación Legal de Comunicaciones.
- 3.6. Adquisición de Chats y Mensajería Instantánea.

UNIDAD 4: PROTOCOLO DE ADQUISICION DIRECTA

- 4.1. Las formas de obtención de la Evidencia. El *corpus instrumentorum*.
- 4.2. El Allanamiento. El Secuestro. La Requisa. La Interceptación.
- 4.3. La Cadena de Custodia en la Evidencia Digital Perdurable.
- 4.4. La Cadena de Custodia en la Evidencia Digital Volátil.
- 4.5. Casos de Análisis Previo a la Adquisición. Contaminación.
- 4.6. Problemas en la Identificación y Adquisición : Herramientas Antiforenses. Rootkits.

UNIDAD 5: ADQUISICION INDIRECTA DE EVIDENCIA DIGITAL

- 5.1. La Escena del Crimen moderna. Globalización. Alcances.
- 5.2. Evidencia fuera de la Escena del Crimen y conservada por terceros.
- 5.3. Las Instituciones Contraloras y Superintendencias. Las Empresas Financieras y de Telecomunicaciones. Obligatoriedad de brindar información. El Decreto Ley 15.322
- 5.4. El equilibrio entre Privacidad e Información.-
- 5.5. Utilización de Recursos Internacionales : MLAT, INTERPOL, FBI.
- 5.6. Pericia en el Extranjero. Validación. Admisibilidad.

III. METODOLOGIA DEL TALLER.

El taller es Teórico – Práctico.

Cada Unidad se desarrolla con una Práctica de lo avanzado, en forma interactiva, antes de avanzar a la siguiente Unidad.

Las últimas 6 horas del Taller, son de práctica Intensiva.

IV. EVALUACIÓN DE LA CAPACITACION.

La Evaluación Sumativa se realizará a la conclusión de de la Capacitación, ocupando la última hora/reloj de las planificadas.

V. BIBLIOGRAFIA BASICA.

- CASEY, Eoghan “Manual de Investigación en Crimen Computacional. Herramientas Forenses y Tecnología”, San Diego: Academic Press, 2002
- Constitución de la República de Uruguay, Código Penal, Códigos de Proceso Penal y General. Leyes
- MENDELL, Ronald “Computer Crime Investigator's Toolkit”
- CANO, J. (2006b) Introducción a la informática forense. Una disciplina técnico-legal. *Revista SISTEMAS*. Asociación Colombiana de Ingenieros de Sistemas – ACIS. No. 96. Disponible en: <http://www.acis.org.co> , Sección **Publicaciones**, Sección **Revista Sistemas**.

- Guidelines for the Management of IT Evidence. HB:171 2003. Standards Australia International Ltd.
- Departamento de Justicia de Estados Unidos “ Electronic Crime Scene Investigation: A Guide for First Responders”, Office of Justice Programs, 2001
- RUIBIN, Gong & CHAN KAI YUN, Tony “ Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework ”, School of Computer Engineering, Nanyang Technological University, Singapore, 2005
- Papers, Conferencias y Trabajos de Investigación presentados por el Autor en Diferentes Congresos y Cursos a nivel Nacional e Internacional.

Duración:

16 hs. Teórico-Prácticas presenciales.

Materiales a Entregar:

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

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.
- Cursado previo de **Pericia Informática Forense I (Curso Básico)**, con preferencia.

Audiencia:

- Gerentes de IT, (CIOs y CISOs.), Ingenieros de Sistemas e Informática noveles en búsqueda de definición de Especialidad en área Forense.
- Peritos Informáticos, Peritos Auditores y Contadores Forenses o en proceso de especialización Forense.
- Fiscales y Abogados en Función de Administración de Justicia
- Abogados en Ejercicio libre. Consorcios Jurídicos de Asesoría.
- Policía Nacional. Grupos Especiales. Miembros de Laboratorio y Escena del Crimen. Investigadores de FELCC.
- Personal de Administración de Justicia en general.

Instructor:

Flavio H. Díaz Portela, CIA Bolivia.