

EVIDENCIAS ELECTRÓNICAS EN LA INVESTIGACIÓN DE DELITOS

Taller para la Región de Centroamérica del Grupo de Trabajo OEA-REMJA sobre Delito Cibernético

Ciudad de Panamá, Panamá

Del 25 al 27 de agosto de 2009

Martes, 25 de agosto

8:30 Llegada e inscripciones

9:00 **Sesión de apertura**

Bienvenida y presentación de los representantes de Panamá, Estados Unidos y de la Organización de los Estados Americanos

10:00 Receso

10:20 **Investigaciones con computadoras e “Internet”**

Albert Rees

Fiscal

*Departamento de
Justicia de Estados
Unidos*

Es posible que existan evidencias electrónicas de la mayoría de los delitos.

- Naturaleza y ubicación de las evidencias electrónicas
- Panorama general de las investigaciones con evidencias electrónicas
- Papel de los investigadores, analistas y fiscales
- Capacitación básica y equipo para la policía e investigadores

11:00 **Sesión plenaria: consideraciones jurídicas para la recopilación de evidencias electrónicas**

Las leyes sientan las bases para que los investigadores recopilen evidencias

- Los participantes expondrán la normativa y procedimientos de sus países para recopilar evidencias y su efecto en la recopilación de evidencias electrónicas
- Describirán la normatividad jurídica de sus países para lograr sentencias condenatorias mediante el uso de evidencias electrónicas
- Se invita a todos a presentar ejemplos de sus países sobre sus experiencias positivas y retos en el uso de evidencias electrónicas en procesos jurídicos

11:40 **Computadoras, redes e “Internet”**

Luis A. Gorgona S.

*Subdirector de
Tecnología de la
Información del
Ministerio de la
Presidencia de Costa
Rica*

Una introducción a los sistemas de computadoras y cómo funciona la “Internet”

- Creación y almacenamiento de información
- Envío de información a través de “Internet” direcciones IP (“Internet protocol”)
- Aplicaciones de “Internet”: correo electrónico y exploradores

13:00 Almuerzo

14:00 **Primera respuesta: antes de que llegue la policía**

Luis A. Gorgona S.

*Subdirector de
Tecnología de la
Información del
Ministerio de la
Presidencia de Costa
Rica*

Muchas cosas habrán ocurrido antes de que se dé parte a la policía de un delito en el que están relacionadas las computadoras o la “Internet”

- El papel del administrador de sistemas en la respuesta a un incidente
- Funciones y papel del CSIRT
- Los objetivos de la respuesta a incidentes
- Ayuda al cumplimiento de las leyes en las investigaciones

15:00	Primera respuesta: etapas iniciales de la investigación	Matt Ralls <i>Agente Especial Servicio Secreto de los Estados Unidos</i>
	Los investigadores deben responder de inmediato para identificar y salvaguardar las evidencias electrónicas <ul style="list-style-type: none"> • Entrevista a los administradores de sistemas y otros testigos • Identificación de fuentes de evidencias electrónicas y de otro tipo • Preservación de las evidencias electrónicas • Integración de evidencias electrónicas y de otro tipo en la investigación • Gestión de casos y plan de investigación 	
16:00	Receso	
16:20	Introducción a un caso práctico	Michelle Kane <i>Fiscal Departamento de Justicia de Estados Unidos</i>
	Los participantes se dividirán en grupos con el objetivo de estudiar un caso hipotético relacionado con computadoras e “Internet” y aplicar los principios presentados en el taller	
16:30	Debates en grupos: evidencias en formato digital y elaboración de un plan de investigación	
17:30	Fin de actividades del día	

Miércoles, 26 de agosto

9:00	Sesión plenaria: acciones de primera respuesta y plan de investigación	
	Los participantes darán un informe del debate que tuvieron en grupos el día anterior e incluirán sus conclusiones, acciones propuestas y puntos sin resolver	
9:30	Recopilación de evidencias en formato digital: investigaciones con correo electrónico []	
	Los mensajes de correo electrónico pueden ser una fuente de evidencias sobre cualquier delito <ul style="list-style-type: none"> • Componentes de los mensajes de correo electrónico • Encabezados de mensajes electrónicos y otros metadatos • Rastreo de mensajes electrónicos • Colaboración con proveedores de servicio que conservan datos y registros • Asuntos internacionales 	
10:30	Receso	
10:50	Recopilación de evidencias en formato digital: investigaciones en línea	Matt Ralls
	Las personas que utilizan la “Internet” dejan evidencias que pueden ser difíciles de seguir pero que resultan ser valiosas <ul style="list-style-type: none"> • Aplicaciones comunes: páginas web, IRC, IM, P2P, VOIP • Reconocimiento en línea • Codificación • Protección de la identidad en línea del investigador • Colaboración con proveedores de servicio • Asuntos internacionales 	

13:00 Almuerzo

14:00 **Recopilación de evidencias en formato digital: computadoras, redes y equipo conexo** Matt Ralls

Las computadoras y otros dispositivos electrónicos pueden contener un sinnúmero de información

- Búsqueda y confiscación de computadores y evidencias conexas
- Preparación de la búsqueda y confiscación; reconocimiento y planificación
- Protección de computadoras para análisis y preservación de datos
- Recopilación (clasificación) inicial de datos; recopilación de datos volátiles
- Asistencia del analista forense y del administrador de sistemas
- Procesamiento de imágenes y preservación de evidencias
- Recopilación y uso de evidencias no electrónicas

15:00 **Informática forense**

[]

Una introducción a la informática forense para investigadores y fiscales, y las evidencias obtenidas a través del análisis

- Descripción de la informática forense
- Lo que la informática forense puede dar al investigador y al fiscal; lo que no puede dar
- Técnicas comunes
- Colaboración con el analista forense

16:00 Receso

16:20 **Debates en grupos: recopilación de evidencias en formato digital y creación de un cronograma**

17:30 Fin de actividades del día

Jueves, 27 de agosto

9:00 **Sesión plenaria: recopilación de evidencias en formato digital y creación de un cronograma**

Los participantes darán un informe del debate que tuvieron en grupos el día anterior e incluirán sus conclusiones, acciones propuestas y puntos sin resolver

9:30 **Cooperación internacional:**

Albert Rees

La naturaleza internacional de la "Internet" requiere una nueva forma de pensar en la cooperación internacional.

- Aplicación de principios de asistencia jurídica internacional a las evidencias electrónicas
- Necesidad de leyes y procedimientos armonizados: Convención sobre Delitos Cibernéticos
- Preservación de datos y la Red 24/7
- Algunas soluciones; problemas continuos

10:30 Receso

10:50	Teléfonos móviles como evidencia electrónica	Matt Ralls
	<p>Los teléfonos móviles, presentes por todos lados, pueden ser una importante fuente de evidencias</p> <ul style="list-style-type: none"> • Evidencias en los teléfonos móviles • Búsqueda y confiscación de teléfonos móviles • Evidencias que conservan los proveedores de servicios • Ubicación de los teléfonos móviles 	
12:00	Atribución de usuarios	Michelle Kane
	<p>Los investigadores y fiscales deben demostrar que el sospechoso utilizó la computadora.</p> <ul style="list-style-type: none"> • Uso de evidencias electrónicas y de otro tipo para demostrar que una persona utilizó una computadora en determinado momento y lugar • Réplica a las explicaciones de los sospechosos de que no se trataba de ellos 	
13:00	Almuerzo	
14:00	El Grupo de Trabajo en Delito Cibernético de la OEA	Rodrigo Cortés <i>Oficial Jurídico</i> <i>Departamento de</i> <i>Cooperación Jurídica</i> <i>Secretaría de Asuntos</i> <i>Jurídicos de la OEA</i>
	Este grupo de expertos gubernamentales tiene responsabilidades en este campo o en materia de cooperación internacional para la investigación y persecución del delito cibernético, de los Estados Miembros de la OEA.	
14:30	Sesión plenaria: reunión de todas las evidencias y preparación para el juicio	Michelle Kane
	Los participantes y moderadores compartirán sus requerimientos, prácticas y experiencias para llevar una investigación a su término, preparar el proceso y la conclusión satisfactoria de un juicio.	
15:30	Conclusión del taller y comentarios	
16:00	Clausura	
17:00	Conclusión del taller	

Información sobre este taller y otros programas sobre delitos cibernéticos de la OEA-REMJA:

Departamento de Cooperación Jurídica
Secretaría de Asuntos Jurídicos
Organización de los Estados Americanos

Rodrigo Cortés: rcortes@oas.org
+1 (202) 458-3395

www.oas.org/juridico/spanish/
www.oas.org/juridico/english/

Sección sobre Delitos Cibernéticos y Propiedad Intelectual
División de Derecho Penal
Departamento de Justicia de Estados Unidos

Albert Rees: albert.rees@usdoj.gov
Jaikumar Ramaswamy: jaikumar.ramaswamy@usdoj.gov
+1 (202) 514-1026
www.cybercrime.gov