UNIVERSIDAD PARAGUAYO ALEMANA

Ingeniería en Tecnologías de la Información Empresarial TIE

Seguridad en TICs

Prof.: Chrystian Ruiz Diaz

DISCLAIMER

Todo el contenido de esta presentación se proporciona **exclusivamente con fines didácticos y educativos en el ámbito académico**.

El uso inapropiado de las técnicas y/o conocimientos expuestos en esta presentación puede violar leyes nacionales e internacionales.

El autor y la institución educativa no se hacen responsables del uso indebido de la información contenida en esta presentación.

Se enfatiza que la información debe ser empleada únicamente para propósitos éticos, legales y con la debida autorización de las autoridades competentes.

Técnicas de Búsqueda y Decomiso para las Escenas de Crímenes Digitales

Principios del Peritaje

1. **OBJETIVIDAD**: El perito debe ser objetivo, debe observar los códigos de ética profesional.
2. **AUTENTICIDAD Y CONSERVACIÓN**: Durante la investigación, se debe conservar la autenticidad e integridad de los medios probatorios
3. **LEGALIDAD**: El perito debe ser preciso en sus observaciones, opiniones y resultados, conocer la legislación respecto de sus actividad pericial y cumplir con los requisitos establecidos por ella
4. **IDONEIDAD**: Los medios probatorios deben ser auténticos, ser relevantes y suficientes para el caso.
5. **INALTERABILIDAD**: En todos los casos, existirá una cadena de custodia debidamente asegurada que demuestre que los medios no han sido modificados durante la pericia.
6. **DOCUMENTACIÓN**: Deberá establecerse por escrito los pasos dados en el procedimiento pericial

Técnicas de Búsqueda y Decomiso para las Escenas de Crímenes Digitales

Reconocimiento de la Evidencia Digital

Es importante **clarificar los conceptos y describir la terminología adecuada** que nos señale el rol que tiene un sistema informático dentro del *iter criminis* o camino del delito. Ej el procedimiento para obtención de la información para un homicidio será totalmente diferente al de un fraude. En esencia se debe identificar el **¡Donde debe ser ubicada!** y como **!debe ser usada la evidencia!**

Categorías

Evidencia Electrónica: elemento material de un sistema informático o hardware

Evidencia Digital: es la información contenida en la evidencia electrónica

Técnicas de Búsqueda y Decomiso para las Escenas de Crímenes Digitales

Reconocimiento de la Evidencia Digital

Hardware o Elementos Físicos

- El hardware es mercancía ilegal o fruto del delito. Ej.: Decodificadores de la señal de televisión por cable, su posesión es una **violación a los derechos de propiedad intelectual** y también un delito.
- Es un instrumento cuando el hardware cumple un papel importante en el cometimiento del delito, podemos decir **que es usada como un arma o herramienta**, tal como una pistola o un cuchillo. Ej *Sniffers*
- El hardware **como evidencia**; es un elemento físico que se constituye como prueba de la comisión de un delito. Ej.: escáner para digitales imágenes prohibidas.

Técnicas de Búsqueda y Decomiso para las Escenas de Crímenes Digitales

Reconocimiento de la Evidencia Digital

Evidencia Digital

- La información **es considerada como mercancía ilegal** cuando su posesión **no está permitida** por la ley. Ej.: secretos industriales, pornografía infantil, copias pirateadas.
- La información es un instrumento o herramienta cuando es usada como medio para cometer una infracción penal. Ej programas para romper las seguridades de un sistema informático.
- La información es evidencia: muchas de nuestras acciones diarias dejan un rastro digital. Ej información de los ISP, Bancos

Técnicas de Búsqueda y Decomiso para las Escenas de Crímenes Digitales

Clases de Equipos Informáticos y Electrónicos

1. **SISTEMAS DE COMPUTACIÓN ABIERTOS**, son aquellos que están compuestos de las llamadas computadores personales y todos sus periféricos como teclados, ratones y monitores, las computadoras portátiles, y los servidores. Actualmente estos computadores tiene la capacidad de guardar gran cantidad de información dentro de sus discos duros, lo que los convierte en una gran fuente de evidencia digital
2. **SISTEMAS DE COMUNICACIÓN**, estos están compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y el Internet. Son también una gran fuente de información y de evidencia digital.
3. **SISTEMAS CONVERGENTES DE COMPUTACIÓN**, son los que están formados por los teléfonos celulares llamados inteligentes o SMARTPHONES, los asistentes personales digitales PDAs, las tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que puede contener evidencia digital

Técnicas de Búsqueda y Decomiso para las Escenas de Crímenes Digitales

Dada la ubicuidad de la evidencia digital es raro el delito que no esté asociado a un mensaje de datos guardado y trasmitido por medios informáticos

Ø Computador de escritorio, Computador Portátil
Ø Estación de Trabajo
Ø Hardware de Red
Ø Servidor – aparato que almacena o transfiere datos electrónico por el Internet
Ø Teléfono celular, Teléfono inalámbrico
Ø Aparato para identificar llamadas
Ø Localizador - beeper
Ø "GPS" – aparato que utiliza tecnología satélite capaz de ubicar geográficamente a la persona o vehículo que lo opera
Ø Cámaras, videos
Ø Sistemas de seguridad
Ø Memoria "flash"

Ø Juegos electrónicos – en su unidad de datos se puede guardar, incluso, una memoria de otro aparato
Ø Sistemas en vehículos – computadoras obvias y computadoras del sistema operativo del vehículo que registra cambios en el ambiente y el mismo vehículo
Ø Impresora, Copiadora, Grabadora, Videograbadora, DVD
Ø Duplicadora de discos
Ø Discos, disquetes, cintas magnéticas
Ø Aparatos ilícitos – tales como los aparatos que capturan el número celular de teléfonos cercanos para después copiarlo en otros teléfonos, o los llamados sniffers, decodificadores, etc.

Técnicas de Búsqueda y Decomiso para las Escenas de Crímenes Digitales

Incautación de Equipos Informáticos o Electrónicos

Si el investigador presume que existe algún tipo evidencia digital en algún aparato electrónico o en algún otro soporte material relacionado con el cometimiento de una infracción. Este debe pedir la correspondiente **autorización judicial para incautar dichos elementos**, de igual forma debe tener la autorización judicial para acceder al contenido guardado, almacenado y generado por dichos aparatos

Técnicas de Búsqueda y Decomiso para las Escenas de Crímenes Digitales

Incautación de Equipos Informáticos o Electrónicos

Consideraciones previas (11) para realizar la incautación:

1. ¿A qué horas debe realizarse?

- ✓ Para minimizar destrucción de equipos, datos
- ✓ El sospechoso tal vez estará en línea
- ✓ Seguridad de investigadores

2. Entrar sin previo aviso

- ✓ Utilizar seguridad
- ✓ Evitar destrucción y alteración de los equipos, o la evidencia contenida en esta.

3. Materiales previamente preparados (Cadena de custodia)

- ✓ Embalajes de papel
- ✓ Etiquetas
- ✓ Discos y disquetes vacíos
- ✓ Herramienta
- ✓ Cámara fotográfica

4. **Realizar simultáneamente los allanamientos e incautación en diferentes sitios**

- ✓ Datos pueden estar en más de un lugar, sistemas de red, conexiones remotas.

5. Examen de equipos

6. Aparatos no especificados en la orden de allanamiento

7. Creación de Respaldos en el lugar, creación de imágenes de datos.

- ✓ Autorización para duplicar, reproducir datos encontrados (por ejemplo, un aparato contestador)

8. Fijar/grabar la escena

- ✓ Cámaras, videos, etiquetas

Técnicas de Búsqueda y Decomiso para las Escenas de Crímenes Digitales

Incautación de Equipos Informáticos o Electrónicos

Consideraciones previas para realizar la incautación:

9. Códigos/claves de acceso/contraseñas
10. Buscar documentos que contienen información de acceso, conexiones en redes, etc.
11. Cualquier otro tipo de consideración especial (consideraciones de la persona involucrada: médicos, abogados, información privilegiada, etc.)

La falta de una orden de allanamiento e incautación que ampare las actuaciones (sobre los equipos y sobre la información) de la Policía Judicial y la Fiscalía **puede terminar con la exclusión de los elementos probatorios por violación de las Garantías Constitucionales**

Técnicas de Búsqueda y Decomiso para las Escenas de Crímenes Digitales

En la Escena del Delito

Responsabilidades del Investigador (9)

1- Observe y Establezca los Parámetros de la Escena del Delito: El primero en llegar a la escena, debe establecer si el delito está todavía en progreso, luego tiene que tomar nota de las características físicas del área circundante. Para los investigadores forenses esta etapa debe ser extendida a todo sistema de información y de red que se encuentre dentro de la escena. En estos casos dicho sistema o red pueden ser blancos de un inminente o actual ataque como por ejemplo uno de denegación de servicio (DoS).

Técnicas de Búsqueda y Decomiso para las Escenas de Crímenes Digitales

En la Escena del Delito

Responsabilidades del Investigador

2 - Inicie las Medidas de Seguridad: El objetivo principal en toda investigación es la seguridad de los investigadores y de la escena. Si uno observa y establece en una condición insegura dentro de una escena del delito, debe tomar las medidas necesarias para mitigar dicha situación. Se deben tomar las acciones necesarias a fin de evitar riesgos eléctricos, químicos o biológicos, de igual forma cualquier actividad criminal. Esto es importante ya que en una ocasión en una investigación de pornografía infantil en Estados Unidos un investigador fue muerto y otro herido durante la revisión de una escena del crimen.

Técnicas de Búsqueda y Decomiso para las Escenas de Crímenes Digitales

En la Escena del Delito

Responsabilidades del Investigador

3- Facilite los Primeros Auxilios: Siempre se deben tomar las medidas adecuadas para precautelar la vida de las posibles víctimas del delito, el objetivo es brindar el cuidado médico adecuado por el personal de emergencias y el preservar las evidencias.

4- Asegure Físicamente la Escena: Esta etapa es crucial durante una investigación, se debe retirar de la escena del delito a todas las personas extrañas a la misma, el objetivo principal es el prevenir el acceso no autorizado de personal a la escena, evitando así la contaminación de la evidencia o su posible alteración.

Técnicas de Búsqueda y Decomiso para las Escenas de Crímenes Digitales

En la Escena del Delito

Responsabilidades del Investigador

5 - Asegure Físicamente las Evidencias: Este paso es muy importante a fin de mantener la cadena de custodia de las evidencias, se debe guardar y etiquetar cada una de ellas. En este caso se aplican los principios y la metodología correspondiente a la recolección de evidencias de una forma práctica. Esta recolección debe ser realizada por personal entrenado en manejar, guardar y etiquetar evidencias.

6 - Entregar la Escena del Delito: Después de que se han cumplido todas las etapas anteriores, la escena puede ser entregada a las autoridades que se harán cargo de la misma. Esta situación será diferente en cada caso, ya que por ejemplo en un caso penal será a la Policía Judicial o al Ministerio Público; en un caso corporativo a los Administradores del Sistema. Lo esencial de esta etapa es verificar que todas las evidencias del caso se hayan recogido y almacenado de forma correcta, y que los sistemas y redes comprometidos pueden volver a su normal operación.

Técnicas de Búsqueda y Decomiso para las Escenas de Crímenes Digitales

En la Escena del Delito

Responsabilidades del Investigador

7 - Elaborar la Documentación de la Explotación de la Escena: Es Indispensable para los investigadores documentar cada una de las etapas de este proceso, a fin de tener una completa bitácora de los hechos sucedidos durante la explotación de la escena del delito, las evidencias encontradas y su posible relación con los sospechosos. Un investigador puede encontrar buenas referencias sobre los hechos ocurridos en las notas recopiladas en la explotación de la escena del Delito.

Técnicas de Búsqueda y Decomiso para las Escenas de Crímenes Digitales

Reconstrucción de la Escena del Delito

La reconstrucción del delito permite al investigador forense comprender todos los hechos relacionados con el cometimiento de una infracción, usando para ello las evidencias disponibles. Los indicios que son utilizados en la reproducción del Delito permiten al investigador realizar tres formas de reconstrucción a saber:

· ***Reconstrucción Relacional***, se hace en base a indicios que muestran la correspondencia que tiene un objeto en la escena del delito y su relación con los otros objetos presentes. Se busca su interacción en conjunto o entre cada uno de ellos;

· ***Reconstrucción Funcional***, se hace señalando la función de cada objeto dentro de la escena y la forma en que estos trabajan y como son usados;

· ***Reconstrucción Temporal***, se hace con indicios que nos ubican en la línea temporal del cometimiento de la infracción y en relación con las evidencias encontradas.

Técnicas de Búsqueda y Decomiso para las Escenas de Crímenes Digitales

Qué hacer al encontrar un dispositivo informático o electrónico

- ✓ No tome los objetos sin guantes de hule, podría alterar, encubrir o hacer desaparecer las huellas dactilares existentes en el equipo o en el área donde se encuentra residiendo el sistema informático.
- ✓ Asegure el lugar.
- ✓ Asegure los equipos. De cualquier tipo de intervención física o electrónica hecha por extraños.
- ✓ Si no está encendido, no lo encienda (para evitar el inicio de cualquier tipo de programa de autoprotección
- ✓ Verifique si es posible el Sistema Operativo a fin de iniciar la secuencia de apagado a fin de evitar pérdida de información.
- ✓ Si usted cree razonablemente que el equipo informático o electrónico está destruyendo la evidencia, debe desconectarlo inmediatamente.
- ✓ Si está encendido, no lo apague inmediatamente (para evitar la pérdida de información “volátil”)

Técnicas de Búsqueda y Decomiso para las Escenas de Crímenes Digitales

REGLA DEL ENCENDIDO “ON” Y APAGADO “OFF”

1. Si el aparato está encendido "ON", no lo apague "OFF".

- ✓ Si lo apaga "OFF" puede iniciarse el bloqueo del aparato.
- ✓ Transcriba toda la información de la pantalla del aparato y de ser posible tómele una fotografía.
- ✓ Vigile la batería del aparato, el transporte del mismo puede hacer que se descargue. Tenga a mano un cargador
- ✓ Selle todas las entradas y salidas.
- ✓ Selle todos los puntos de conexión o de admisión de tarjetas o dispositivos de memoria
- ✓ Selle los tornillos para evitar que se puedan retirar o reemplazar piezas internas.
- ✓ Buscar y asegurar el conector eléctrico.

Técnicas de Búsqueda y Decomiso para las Escenas de Crímenes Digitales

REGLA DEL ENCENDIDO “ON” Y APAGADO “OFF”

- ✓ Colocar en una bolsa de FARADAY, (especial para aislar de emisiones electromagnéticas), si no hubiere disponible, en un recipiente vacío de pintura con su respectiva tapa.
- ✓ Revise los dispositivos de almacenamiento removibles. (Algunos aparatos contienen en su interior dispositivos de almacenamiento removibles tales como tarjetas SD, Compact flash, Tarjetas XD, Memory Stick, etc.)

2. Si el aparato está apagado "OFF", déjelo apagado "OFF".

- ✓ Prenderlo puede alterar evidencia al igual que en las computadoras.
- ✓ Es necesario que el investigador busque el manual del usuario relacionado con el aparato encontrado.

Casos de Uso

- **Investigaciones Criminales: Cibercrimen, fraude, acoso en línea.**
- **Auditorías de Seguridad: Evaluación de brechas de seguridad.**
- **Análisis de Malware: Identificación y estudio de software malicioso.**

Desafíos en el Análisis Forense Digital

- **Volumen de Datos**: Manejo de grandes cantidades de información.
- **Encriptación**: Dificultad para acceder a datos cifrados.
- **Evolución Tecnológica**: Rápido cambio en tecnologías y métodos de ataque.

Conclusión

El análisis forense digital es crucial para la seguridad y la justicia en el mundo digital.

Futuro

La importancia del análisis forense digital seguirá creciendo con el aumento de la digitalización y los ciberataques.

Referencias

- Vieites, Á. G. (2014). Gestión de incidentes de seguridad informática. RA-MA Editorial.
- OAS. (07 de 05 de 2021). Organization of American States. Obtenido de https://www.oas.org/juridico/english/cyb_pan_manual.pdf

¿PREGUNTAS?

Actividad de Laboratorio

Muchas Gracias..!!