INTRODUCCIÓN A LA INFORMÁTICA FORENSE

Dr. Santiago Acurio Del Pino

Agenda

- Prueba de los Delitos Informáticos
- Informática Forense
- En la escena del Delito
- Roles de la Investigación
- Caso Práctico

Prueba de los Delitos Informáticos

Evidencia Digital, Reconocimiento de la Evidencia

Evidencia electrónica

Prueba de los Delitos Informáticos

- La prueba dentro del proceso penal es de especial importancia, ya que desde ella se confirma o desvirtúa una hipótesis o afirmación precedente, se llega a la posesión de la verdad material.
- De esta manera se confirmará la existencia de la infracción y la responsabilidad de quienes aparecen en un inicio como presuntos responsables, todo esto servirá para que el Tribunal de Justicia alcance el conocimiento necesario y resuelva el asunto sometido a su conocimiento.

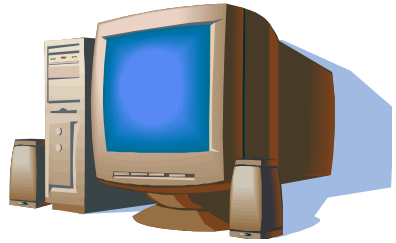
Reconocimiento de la Evidencia Digital

- 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.
- Esto a fin de encaminar correctamente el tipo de investigación, la obtención de indicios y posteriormente los elementos probatorios necesarios para sostener nuestro caso.
- Es así que por ejemplo, el procedimiento de una investigación por homicidio que tenga relación con evidencia digital será totalmente distinto al que, se utilice en un fraude informático, por tanto el rol que cumpla el sistema informático determinara DONDE DEBE SER UBICADA Y COMO DEBE SER USADA LA EVIDENCIA.

Reconocimiento de la Evidencia Digital

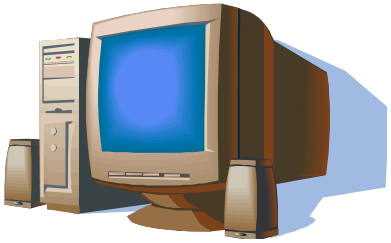
- Ahora bien para este propósito se han creado categorías a fin de hacer una necesaria distinción entre el elemento material de un sistema informático o hardware (evidencia electrónica) y la información contenida en este (evidencia digital).
- Esta distinción es útil al momento de diseñar los procedimientos adecuados para tratar cada tipo de evidencia y crear un paralelo entre una escena física del crimen y una digital.
- En este contexto el hardware se refiere a todos los componentes físicos de un sistema informático, mientras que la información, se refiere a todos los datos, programas almacenados y mensajes de datos trasmitidos usando el sistema informático.

Elementos Físicos



SISTEMA INFORMÁTICO	
HARDWARE (Elementos Físicos)	**Evidencia Electrónica**
• El hardware es mercancía ilegal o fruto del delito.	• El hardware es una mercancía ilegal cuando su posesión no está autorizada por la ley. Ejemplo: en el caso de los decodificadores de la señal de televisión por cable, su posesión es una violación a los derechos de propiedad intelectual y también un delito. • El hardware es fruto del delito cuando este es obtenido mediante robo, hurto, fraude u otra clase de infracción.
• El hardware es un instrumento	• 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. Un ejemplo serían los snifers y otros aparatos especialmente diseñados para capturar el tráfico en la red o interceptar comunicaciones.
• El hardware es evidencia	• En este caso el hardware no debe ni ser una mercancía ilegal, fruto del delito o un instrumento. Es un elemento físico que se constituye como prueba de la comisión de un delito. Por ejemplo el scanner que se uso para digitalizar una imagen de pornografía infantil, cuyas características únicas son usadas como elementos de convicción

Información



SISTEMA INFORMÁTICO	
INFORMACIÓN	**Evidencia Digital**
• La información es mercancía ilegal o el fruto del delito.	La información es considerada como mercancía ilegal cuando su posesión no está permitida por la ley, por ejemplo en el caso de la pornografía infantil. De otro lado será fruto del delito cuando sea el resultado de la comisión de una infracción, como por ejemplo las copias pirateadas de programas de ordenador, secretos industriales robados.
• La información es un instrumento	La información es un instrumento o herramienta cuando es usada como medio para cometer una infracción penal. Son por ejemplo los programas de ordenador que se utilizan para romper las seguridades de un sistema informático, sirven para romper contraseñas o para brindar acceso no autorizado. En definitiva juegan un importante papel en el cometimiento del delito.
• La información es evidencia	Esta es la categoría más grande y nutrida de las anteriores, muchas de nuestras acciones diarias dejan un rastro digital. Uno puede conseguir mucha información como evidencia, por ejemplo la información de los ISP's, de los bancos, y de las proveedoras de servicios las cuales pueden revelar actividades particulares de los sospechosos

Donde buscar la Evidencia: Fuentes de Evidencia

- 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.

Donde buscar la Evidencia: Fuentes de Evidencia

- 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.
- 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.

Propósito de la Clasificación

- En resumen el propósito fundamental de las categorías antes mencionadas es el de enfatizar el papel que juegan los sistemas informáticos en la comisión de delitos, a fin de que el investigador criminal tenga un derrotero claro y preciso al buscar los elementos convicción que aseguren el éxito dentro de un proceso penal.
- En estas condiciones para efectos probatorios son objeto de examen, tanto el hardware como la información contenida en este, para lo cual es necesario contar con el auxilio y el conocimiento que nos brinda la ciencia informática, y en particular de la Ciencia Forense Informática.

Informática forense

Concepto, Dinámica de la Evidencia

Concepto

- Es una ciencia forense que se ocupa de la utilización de los métodos científicos aplicables a la investigación de los delitos, no solo Informáticos y donde se utiliza el análisis forense de las evidencias digitales, en fin toda información o datos que se guardan en una computadora o sistema informático.

- En conclusión diremos que Informática Forense es "*la ciencia forense que se encarga de la preservación, identificación, extracción, documentación y interpretación de la evidencia digital, para luego ésta ser presentada en una Corte de Justicia*".

Evidencia Digital

- En derecho procesal la evidencia es la certeza clara, manifiesta y tan perceptible que nadie puede dudar de ella.
- De otro lado la evidencia digital es cualquier mensaje de datos almacenado y trasmitido por medio de un Sistema de Información que tenga relación con el cometimiento de un acto que comprometa gravemente dicho sistema y que posteriormente guié a los investigadores al descubrimiento de los posibles infractores.
- En definitiva son campos magnéticos y pulsos electrónicos que pueden ser recogidos y analizados usando técnicas y herramientas especiales

Clases de Evidencia Digital

- En un principio el tipo de evidencia digital que se buscaba en los equipos informáticos era del tipo CONSTANTE o PERSISTENTE es decir la que se encontraba almacenada en un disco duro o en otro medio informático y que se mantenía preservada después de que la computadora era apagada.
- Posteriormente y gracias a las redes de interconexión, el investigador forense se ve obligado a buscar también evidencia del tipo VOLÁTIL, es decir evidencia que se encuentra alojada temporalmente en la memoria RAM, o en el CACHE, son evidencias que por su naturaleza inestable se pierden cuando el computador es apagado.
- Este tipo de evidencias deben ser recuperadas casi de inmediato.

Volcado de la memoria global del sistema y de cada proceso

- Volcado de la memoria global del sistema y de cada proceso: ante la dificultad de realizar un análisis en profundidad, se podrá utilizar el volcado de memoria para buscar determinadas cadenas de caracteres que puedan dar pistas sobre el incidente que ha afectado al equipo.

Procesos y Servicios en ejecución dentro del Sistema

- De cada proceso o servicio sería conveniente identificar el archivo ejecutable y los parámetros de ejecución, así como la cuenta de usuario bajo la que se ejecuta, archivos que está usando y qué otro proceso o servicio lo ha llamado (árbol de ejecución), para posteriormente poder comparar esta información con la situación estable del objeto de estudio

Dinámica de la Evidencia

- La dinámica de la evidencia es la forma como se entienden y se describen los diferentes factores (humanos, de la naturaleza, de los equipos) que actúan sobre las evidencias, a fin de determinar los cambios que estos producen sobre ellas.

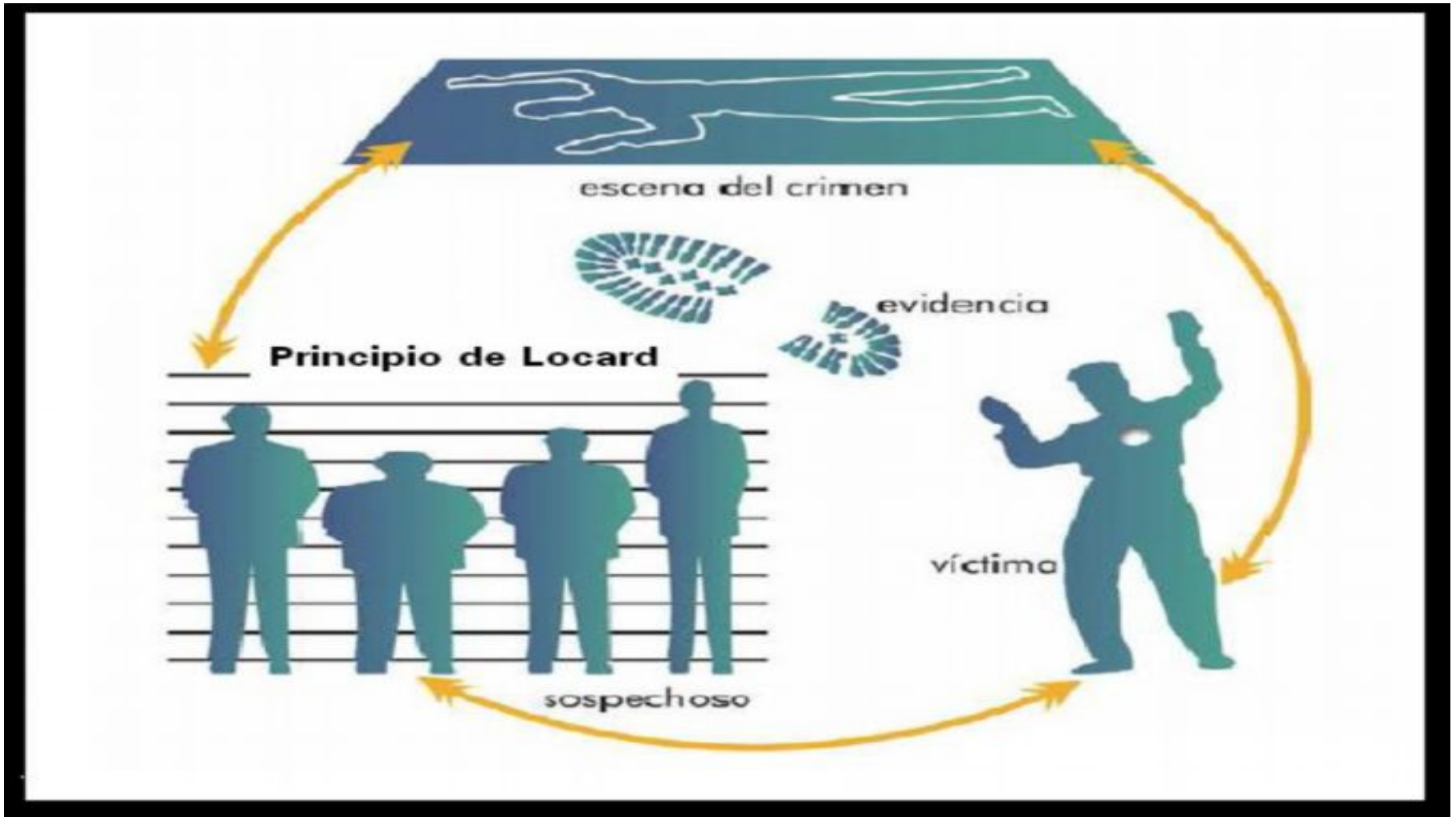
Dinámica de la evidencia

- Podemos afirmar indudablemente que existen muchos agentes que intervienen o actúan sobre la evidencia digital, aquí se aplica el llamado Principio de intercambio o de Locard; el investigador forense se ve en la necesidad de reconocer la forma como estos factores pueden alterar la evidencia, y así tener la oportunidad de manejarla de una manera apropiada, evitando generalmente contaminarla, dañarla y hasta perderla por completo.

Principio de Intercambio

- El principio de intercambio de Locard, menciona que cuando dos objetos entran en contacto siempre existe una transferencia de material entre el uno y el otro.
- Es decir que cuando una persona está en una escena del crimen esta deja algo de si misma dentro de la escena, y a su vez cuando sale de ella esta se lleva algo consigo

Principio de Intercambio



Afectación de la Escena del Crimen: Efectos de la dinámica

- EQUIPOS DE EMERGENCIAS: En el caso de un incendio, los sistemas informáticos pueden ser afectados por el fuego y el humo, posteriormente sometidos a una gran presión de agua al tratar de apagar este. Esto provoca que los técnicos forenses no puedan determinar a ciencia cierta si los sistemas informáticos encontrados en la escena estuvieron comprometidos, fueron atacados o usados indebidamente. En otras ocasiones los equipos de emergencia manipulan la escena cuando es necesario para salvar la vida de una persona.

Afectación de la Escena del Crimen: Efectos de la dinámica

- TESTIGOS: Un administrador del sistema puede borrar cuentas de usuarios sospechosas, las mismas que fueron creadas por un intruso, a fin de prevenir su acceso y utilización futura.
- EL CLIMA Y LA NATURALEZA: Los campos electromagnéticos pueden corromper la información guardada en discos magnéticos.
- DESCOMPOSICIÓN: En algunos casos la información almacenada en discos magnéticos, o en otros soportes puede perderse o tornarse ilegible para los sistemas de información, a causa del tiempo y de las malas condiciones de almacenamiento.

Comprender la Dinámica de la Evidencia

- El investigador forense debe entender como los factores humanos, de la naturaleza y de los propios equipos informáticos pueden alterar, borrar o destruir evidencia,
- Debe comprender como dichas variables actúan sobre la escena misma del delito,
- Debe por tanto encaminar la investigación desde su etapa más temprana tomando en cuenta esos cambios, a fin de adecuar el mejor método para adquirir, preservar y luego analizar las pistas obtenidas, y así reducir de manera considerable los posibles efectos de la dinámica de la evidencia.

En la escena del Delito

Procedimiento de Operaciones Estándar

Procedimiento de Operaciones Estándar

- Cuando se va revisar una escena del crimen del tipo informático es necesario tener en cuenta un procedimiento de operaciones estándar (POE), el mismo que es el conjunto de pasos o etapas que deben realizarse de forma ordenada al momento de recolectar o examinar la evidencia digital.
- Esta serie de procedimientos se utilizan para asegurar que toda la evidencia recogida, preservada, analizada y filtrada se la haga de una manera transparente e integra.
- La transparencia y la integridad metodológica (estabilidad en el tiempo de los métodos científicos utilizados) se requieren para evitar errores, a fin de certificar que los mejores métodos son usados, incrementado cada vez la posibilidad de que dos examinadores forenses lleguen al mismo dictamen o conclusión cuando ellos analicen la misma evidencia por separado. A esto se lo conoce como reexaminación.

Manual de Manejo de Evidencias Digitales y Entornos Informáticos

- Con el propósito de tener una guía de buenas prácticas en la recolección de evidencia digital, la Dirección Nacional de Tecnologías de la Información presento en Junio de este año el Manual de Manejo de evidencias digitales y entornos informáticos V. 2.0 al Señor Fiscal General Dr. Washington Pesantez Muñoz quien con visión de futuro ordeno la impresión de 1600 guías para ser entregadas a todos los funcionarios de la Fiscalía General del Estado.

- El Manual pretende ser una guía de actuación para miembros de la Policía Judicial a si como de los Funcionarios de la Fiscalía General Del Estado, cuando en una escena del delito se encuentren dispositivos Informáticos o electrónicos que estén relacionados con el cometimiento de una infracción de acción pública

Principios Básicos

- El funcionario de la Fiscalía o de la Policía Judicial nunca debe acudir solo al lugar de los hechos, este tipo de actividad debe ser realizada como mínimo por dos funcionarios.
- Un segundo funcionario, por un lado, aporta seguridad personal y, por otro, ayuda a captar más detalles del lugar de los hechos. Los funcionarios deberían planear y coordinar sus acciones.
- Si surgen problemas inesperados, es más fácil resolverlos porque "dos cabezas piensan más que una.

Principios Básicos

- Ninguna acción debe tomarse por parte de la Policía Judicial, Fiscalía o por sus agentes y funcionarios que cambie o altere la información almacenada dentro de un sistema informático o medios magnéticos, a fin de que esta sea presentada fehacientemente ante un tribunal.

Principios Básicos

- En circunstancias excepcionales una persona competente puede tener acceso a la información original almacenada en el sistema informático objeto de la investigación, siempre que después se explique detalladamente y de manera razonada cual fue la forma en la que se produjo dicho acceso, su justificación y las implicaciones de dichos actos.

Principios Básicos

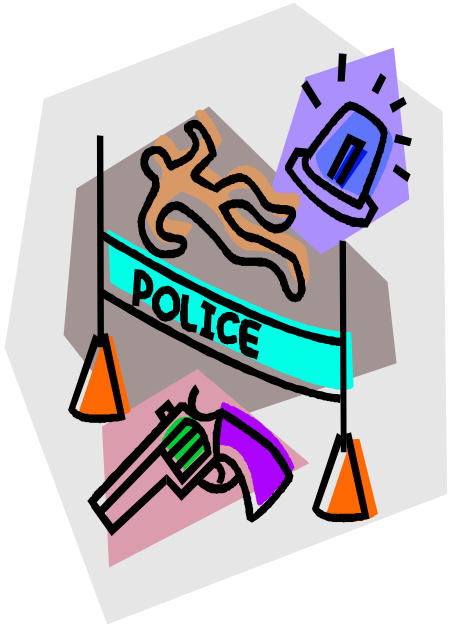
- Se debe llevar una bitácora de todos los procesos adelantados en relación a la evidencia digital. Cuando se hace una revisión de un caso por parte de una tercera parte ajena al mismo, todos los archivos y registros de dicho caso y el proceso aplicado a la evidencia que fue recolectada y preservada, deben permitir a esa parte recrear el resultado obtenido en el primer análisis.

Principios Básicos

- El Fiscal del Caso y/o el oficial a cargo de la investigación son responsables de garantizar el cumplimiento de la ley y del apego a estos principios, los cuales se aplican a la posesión y el acceso a la información almacenada en el sistema informático. De igual forma debe asegurar que cualquier persona que acceda a o copie dicha información cumpla con la ley y estos principios.

Investigación en la escena del Delito

- Observe y establezca los parámetros de la escena del delito: El primero en responder debe establecer si el delito todavía se esta cometiendo, tiene que tomar nota de las características físicas de el 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).



Investigación en la escena del Delito

- 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.

Investigación en la Escena del Delito

- 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.
- 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.

Investigación en la Escena del Delito

- Asegure Físicamente las Evidencias: Este paso es muy importante a fin de mantener la cadena de custodia[1] de las evidencias, se debe guardar y etiquetar cada una de las evidencias. 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.

[1] La cadena de custodia es un sistema de aseguramiento que, basado en el principio de la "mismidad", tiene como fin garantizar la autenticidad de la evidencia que se utilizará como "prueba" dentro del proceso.

Investigación en la escena del Delito

- 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.

Investigación en la Escena del Crimen

- 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.

Reconstrucción de la Escena

- 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.

Reconstrucción de la Escena

- Los indicios que son utilizados en la reproducción del Delito permiten al investigador realizar t res 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.

Roles de la Investigación

Primeros en responder, Peritos, Detectives Digitales

Roles en la Investigación

TÉCNICOS EN ESCENAS DEL CRIMEN INFORMÁTICAS, también llamados FIRST RESPONDENDERS, son los primeros en llegar a la escena del crimen, son los encargados de recolectar las evidencias que ahí se encuentran. Tiene una formación básica en el manejo de evidencia y documentación, al igual que en reconstrucción del delito, y la localización de elementos de convicción dentro de la red.

EXAMINADORES DE EVIDENCIA DIGITAL O INFORMÁTICA, que son los responsables de procesar toda la evidencia digital o informática obtenida por los Técnicos en Escenas del Crimen Informáticos. Para esto dichas personas requieren tener un alto grado de especialización en el área de sistemas e informática.

INVESTIGADORES DE DELITOS INFORMÁTICOS, que son los responsables de realizar la investigación y la reconstrucción de los hechos de los Delitos Informáticos de manera general, son personas que tiene un entrenamiento general en cuestiones de informática forense, son profesionales en Seguridad Informática, Abogados, Policías, y examinadores forenses.

Peritos Informáticos

- Por otro lado, se hace indispensable para la valoración de las pruebas o elementos de convicción la intervención de personas que tengan especiales conocimientos en materias especiales en este caso de la materia informática, personas que prestan un servicio especial al Fiscal y al Juez al momento ilustrar sobre las materias, técnicas o artes que son de su conocimiento, a fin de dichos funcionarios en función de dichas explicaciones puedan emitir su criterio en el momento adecuado (Dictamen Fiscal o la Sentencia)

Peritos Informáticos

- El perito no es mas que un testigo que ha visto los resultados y examinado los rastros materiales: es la mirada del Juez y el Fiscal en esos rastros que requieren algún conocimiento especial propio de su ciencia, arte, profesión u oficio.
- El dictamen del perito debe contener una opinión fundada, exponiendo al juez y al fiscal los antecedentes de orden técnico que tuvo en cuenta, pues, como ya se dijo, su objeto es ilustrar el conocimiento al magistrado y al representante de la Fiscalía General del Estado.
- La pericia, por definición no puede consistir en una mera opinión del experto, prescindiendo del necesario sustento científico

Principios del Peritaje

- Objetividad: El perito debe ser objetivo, debe observar los códigos de ética profesional.
- Autenticidad y conservación: Durante la investigación, se debe conservar la autenticidad e integridad de los medios probatorios
- 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

Principios del Peritaje

- Idoneidad: Los medios probatorios deben ser auténticos, ser relevantes y suficientes para el caso.
- Inalterabilidad: En todos los casos, existirá una cadena de custodia debidamente asegurada que demuestre que los medios no han sido modificados durante la pericia.
- Documentación: Deberá establecerse por escrito los pasos dados en el procedimiento pericial
- Estos principios deben cumplirse en todas las pericias y por todos los peritos involucrados

Formación del Perito Informático

- El Perito Informático Forense según la opinión del Profesor Jeimy Cano[1] requiere la formación de un perito informático integral que siendo especialista en temas de Tecnologías de información, también debe ser formado en las disciplinas jurídicas, criminalisticas y forenses. En este sentido, el perfil que debe mostrar el perito informático es el de un profesional híbrido que no le es indiferente su área de formación profesional y las ciencias jurídicas.

- [1] CANO Jeimy, Estado del Arte del Peritaje Informático en Latinoamérica. ALFA-REDI, 2005

Documentos Informáticos y un caso práctico

Concepto y validez de los documentos

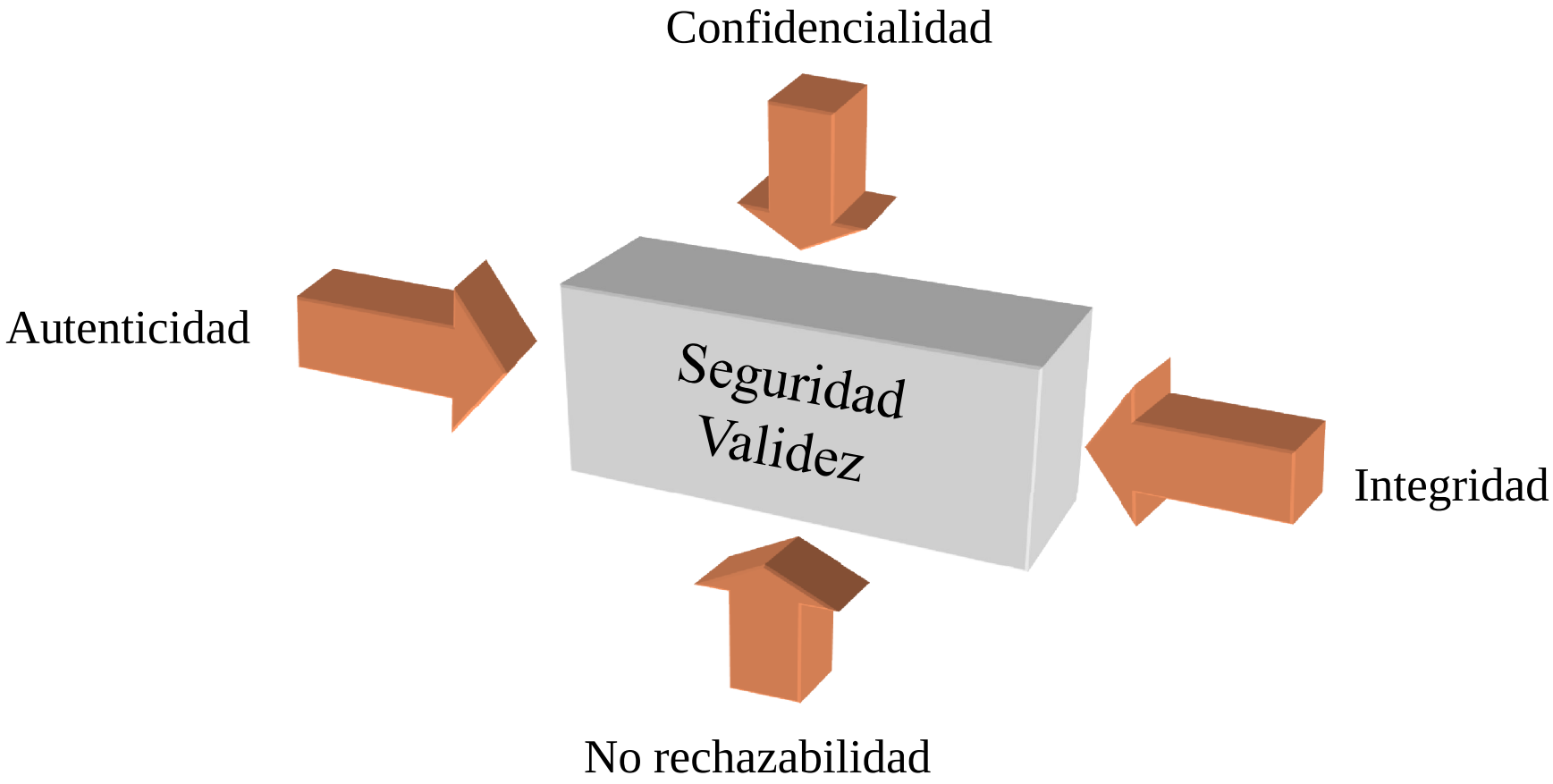
Documentos Informáticos o Electrónicos

- El documento informático puede ser definido como la representación en forma informática de hechos jurídicamente relevantes susceptibles de ser presentados en una forma humanamente comprensible

Validez de los Documentos Electrónicos

- Toda pretensión jurídica dentro de un juicio debe ser sustentada mediante las reglas dadas por el derecho probatorio interno de cada país, ya que de ello depende la efectiva titularidad sobre un derecho discutido o negado.
- Por ello, la prueba se constituye en una de las partes primordiales del proceso y en una condición de seguridad jurídica esencial para el pronunciamiento de una sentencia justa y objetiva.

Validez de los Documentos Electrónicos (comunicaciones electrónicas)



Validez de los Documentos Electrónicos

- Para que un documento electrónico sea válido dentro de un proceso judicial debe tener las siguientes características

  - **Autenticidad**

Capacidad de identificar si determinada persona es el autor de un documento electrónico o si reconoce el contenido del mismo.

  - **Confidencialidad**

Capacidad de mantener un documento electrónico como inaccesible para terceros ajenos a él.

Validez de los Documentos Electrónicos

- Integridad

Capacidad de impedir que un documento electrónico sea alterado en el transcurso de su envío y recepción.

- No Rechazabilidad

Capacidad de impedir que las partes puedan negar haber enviado o recibido un documento electrónico.

Caso Práctico

Caso de Raúl Reyes

Mensajes de Datos

- Fragmento de una de las cartas supuestamente encontradas en las computadoras de Raúl Reyes

ESPERANZA-ENVIADOS.DOC

PARTE DE NY387

Septiembre, 9 de 2006

Camarada Raúl un fuerte abrazo, extensivo para Gloria, Eliana y quienes lc acompañan.

1. De Carlos muchos saludos acompañado de mil disculpas por no haber podido llegar a la cita el día y la hora indicada por motivos de ultima hora, su carro lo chocaron; lo conducía su hermana, afortunadamente para ella no fue mucho el golpe, todo lo recibió el carro que quedo vuelto nada. Propone viajar a su casa el miércoles 13 del presente llegando al sitio a las 10 de la mañana. Si es posible que lo reciba para esa fecha por favor confirmar.

6. Lenin Lara se disculpa no poderlo visitar por motivos de tareas asignadas por su Partido Socialista en este periodo electoral.
7. El general Rene Vargas trabaja en el directorio de PETROECUADOR., Lenir Ortiz trabaja con él. Lenin busco a Lucho para comunicarle que el general desea tener una reunión con usted, según él por su trabajo no puede viajar personalmente propone que viajaría Lenin y otro delegado de la misma compañía. Lenin le comento que esta trabando en la campaña del candidatc presidencial de Rafael Correa. Aproveche que Lucho se reúne con Lenin para que le pida que si es posible una reunión de alto nivel con delegados de Correa, a Lenin le pareció importe y esta trabando en eso.
8. El correo que envió para Lucho, Carlos le entrego pero hubo un error de dedo por parte de Lucho que escribió cordero22 siendo el correcto cardeno22 por eso no le funciono hasta corregir escribió por el anterior.
9. Sobre mi salud, creo que a Carlos que es el que sabe todo sobre el tratamiento que estoy siguiendo según descripción medica le fallaron los cálculos porque esta medicina que me aplican termina en octubre, luego viene una evolución nuevamente del seno izquierdo. En anteriores visitas le envié con el, el informe de los resultado de la biopsia y el tratamiento que el medicc indico.
10. Es todo por ahora. Éxitos en sus tareas diarias. Ana María.

Medio de Prueba de los D.E.

- Mensajes de Datos como medio de prueba
- Medio de Prueba.- procedimiento que establece la Ley para ingresar un elemento de prueba en el proceso
- Art. 53 LCE, Art. 156 del CPP

Admisibilidad de la Evidencia

- Establecer un Procedimiento de Operaciones Estándar
- Cumplimiento de los Principios Básicos
- Cumplir los principios constitucionales y legales (Teoría del Árbol Envenenado, Secreto a la correspondencia y las comunicaciones)
- Seguir el trámite legal

Admisibilidad de la Evidencia

Para esto es necesario probar dos situaciones:

- Debemos establecer que el mensaje de datos usado como evidencia digital fue localizado y recuperado del equipo informático del sospechoso y de ningún otro equipo informático perteneciente a alguien más.

Admisibilidad de la Evidencia

- Debemos comprobar que el mensaje de datos usado como evidencia fue creado o originado en el equipo perteneciente al sospechoso más allá de cualquier duda de que dicho mensaje fue puesto o creado ahí por el equipo informático del investigador

Como se logra la Admisibilidad

- La admisibilidad se logra con la aplicación de los códigos de integridad (Valor HASH) y su comparación
- Es un error verificar la admisibilidad de la evidencia digital (mensajes de Datos) a través de la cadena de custodia.
- La solución es más simple

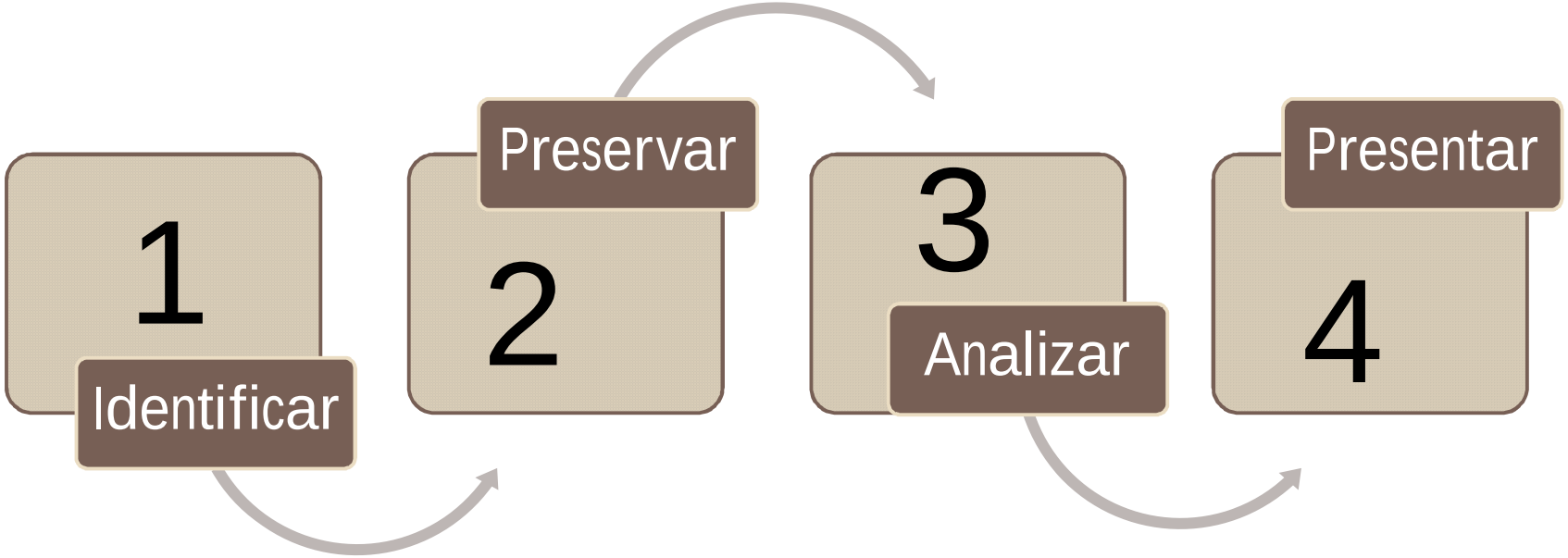
Código de Integridad o Hash

- Es una función matemática que, a partir de un cierto volumen de datos, derivan una pequeña serie de datos, o huella digital.
- 397B3732D63F53BF51FF5210551476F7
- Una función hash comprime los bits del mensaje a un valor hash de tamaño fijado, de manera que distribuye los posibles mensajes uniformemente entre los posibles valores hash.

Caso Reyes

- **Evidencia No. 31**
- Nombre del Archivo: Esperanza-Enviados.doc
- Fecha de Creación: 06/10/07 09:40:38a.m.
- Fecha de Modificación:01/02/07 03:33:20p.m.
- Hash MD5: BB14EF3049F0D11C32692ED42618CE47
- Ruta completa o Path: \comisionInternacional\INTEGRANTES-CMI\AÑO2006\Esperanza-Enviados.doc

Metodología de un Análisis Forense



Preguntas

Muchas Gracias por su atención

Dr. Santiago Acurio Del Pino
Fiscalía General del Estado
sacurio@hotmail.com
acurios@minpec.gov.ec