Introducción

... ...

- Informática
  - Conjunto de conocimientos técnicos que se ocupan del tratamiento automático de la información por medio de computadoras.

Ciencias Forenses

- Antropólogos forenses
- Criminalística
- Medicina forense
- Cómputo forense
- Detección de mentiras
- Odontología forense

Informática Forense

- También llamado cómputo forense, computación forense, análisis forense digital o examinación forense digital.
- Es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.
- Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.
- (Lectura Artículo: La informática forense y los delitos informáticos. Alex Canedo Estrada)

Objetivos

- La compensación de los daños causados por los intrusos o criminales.
- La persecución y procesamiento judicial de los criminales.
- La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos son logrados de varias formas, entre ellas, la principal es la colección de evidencia

Metodología de trabajo

- La metodología de trabajo nos debe garantizar la validación y preservación de los datos que se adquieran en el proceso de análisis forense.
- Los pasos o acciones realizadas, incluyendo posibles modificaciones a cualquier evidencia, se documentan detalladamente.
- Las tareas de investigación se realizan sobre una copia de la información y nunca sobre la evidencia original.
- De hecho, la metodología contempla diversos métodos de adquisición de datos como, por ejemplo, la duplicación de un disco duro.

Metodología del análisis forense

- Identificar
- Preservar
- Analizar
- Presentar

Identificar evidencia

- Según prioridades del cliente
- Conversación inicial

Planeación del proceso que se va a realizar durante la investigación.

Preservar las evidencias

- Fase crítica
- Preservar de forma que no haya duda de la evidencia
- Creación de imágenes a nivel de BIT
- Generar checksum y copias (MD5 y SHA-1)

Analizar las evidencias

- Propósito: Dar respuesta a las preguntas:
  ¿Quién, que, cuando y como?

- Analizar requerimientos del cliente.

Se buscará las evidencias de acuerdo al caso identificado.

Presentación de evidencias

Dar un informe claro, conciso, estructurado y sin ambigüedad de las evidencias.

- No se usará lenguaje muy técnico.
- Deberá contener las evidencias encontradas de acuerdo al caso.

Marco Legal

Triángulo del hecho

Esta relación se establece mediante las evidencias y pruebas electrónicas además de las tradicionales como testificales, documentales, etc.

NCPP: Artículo 76º.- (Víctima)

- A las personas directamente ofendidas por el delito;
- Al cónyuge o conviviente, a los parientes dentro del cuarto grado de consanguinidad o segundo de afinidad, al hijo o padre adoptivo y al heredero testamentario, en los delitos cuyo resultado sea la muerte del ofendido;
- A las personas jurídicas en los delitos que les afecten; y,
- A las fundaciones y asociaciones legalmente constituidas, en aquellos delitos que afecten intereses colectivos o difusos, siempre que el objeto de la fundación o asociación se vincule directamente con estos intereses.

NCPP Artículo 83º.-(Identificación)

- El imputado, desde el primer acto del proceso, será identificado por su nombre, datos personales y señas particulares. Si se abstiene de proporcionar esos datos o los proporciona de manera falsa, se procederá a su identificación por testigos, fotografías, identificación dactiloscópica u otros medios lícitos.

  La duda sobre los datos obtenidos no alterará el curso del proceso y los errores podrán ser corregidos en cualquier oportunidad, aun durante la ejecución penal.

Medios de Prueba

- Testifical (Art. 193 – 203, 350, 351 cpp)
- Pericial (Art. 204 – 215, 349 cpp)
- Documental (Art. 216 – 217 cpp)
- Informes (Art. 218 cpp)
- Careo (Art. 220 cpp)
- Inspección ocular (Art. 179 cpp)
- Reconstrucción de los hechos (Art. 179 cpp)
- Requisa (Art. 175 y 176 cpp)
- Secuestro (Art. 184, 186 cpp)
- Registro del lugar del hecho (Art. 174 cpp)
- Allanamiento (Art. 180, 182 y 183 cpp)

Los artículos actuales que tenemos relacionados a los delitos informáticos:

- Art. 363 bis MANIPULACIÓN INFORMÁTICA
- Art. 363 ter ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS

Art. 363 bis MANIPULACIÓN INFORMÁTICA

- El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de 3ro.

  Sanción: Reclusión 1- 5 años y Multa 60-200 días.

Art. 363 ter ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS

- El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información.

  Sanción: Prestación de Trabajo hasta 1 año o Multa hasta 200 días.

DELITOS INFORMATICOS COMUNES

- MANIPULACION INFORMATICA
  - Robos, hurtos, desfalcos, estafas o fraudes cometidos mediante manipulación de los datos de entrada.
- VIRUS INFORMATICOS
  - Programas generalmente destructivos, con la capacidad de ocultarse, auto reproducirse con múltiples copias y capacidad de propagarse en la Red o por Internet.

DELITOS INFORMATICOS COMUNES

- FRAUDES INFORMATICOS
  - Falsificaciones informáticas que utilizan dispositivos de informática, para producir copias no autorizadas de originales sin autorización del propietario.
- SABOTAJE FÍSICO / LÓGICO
  - (Daños o modificaciones de programas) Daño leve, mediano o mayor a los dispositivos y unidades lógicas de un sistema informático.

DELITOS INFORMATICOS COMUNES

- SUPLANTACION INFORMATICA
  - Falsificaciones informáticas, donde se colocan puntos intermedios disfrazados para burlar controles. Apropiación de Identidades Electrónicas para obtener beneficios personales.
- INTERCEPTACION DE LÍNEAS
  - Pinchado de líneas, interceptación lógica o física de las líneas de telecomunicación y redes para analizar el tráfico y filtrar datos.

DELITOS INFORMATICOS COMUNES

- MODELAMIENTO DE DELITOS
  - Utilizar equipos para simular delitos, copiando sistemas e instalaciones para planificar futuros actos ilícitos.
- INGENIERÍA REVERSA
  - Proceso inverso al armado de programas, transformándolos a código máquina para obtener, vulnerar o romper los códigos, controles de seguridad y protección.

DELITOS INFORMATICOS COMUNES

- ACCESOS SECRETOS ILÍCITOS
  - Superaccesos programados como vías cortas con cuentas de programador. Estableciendo rutinas de facilidad en la administración y puertas secretas.
- PLAGIO Y PIRATERÍA
  - Violación de los Derechos de Propiedad Intelectual en Sw, textos, imágenes y demás contenidos propietarios

DELITOS INFORMATICOS COMUNES

- INVASIÓN A LA PRIVACIDAD
  - Acceso no autorizado a datos personales y su utilización para fines ajenos a los del propietario.
- TERRORISMO INFORMÁTICO
  - Acción orientada a causar temor o daño utilizando los medios informáticos, dañándolos, alterándolos o utilizándolos para fines no especificados en su creación.

DELITOS INFORMATICOS COMUNES

- SPAM
  - Correo comercial no solicitado
- PHISHING
  - Suplantación de Páginas web

Equipo pericial

Para la conformación del equipo pericial tomemos en cuenta lo siguiente:

El delito informático de acuerdo a nuestra ley Art. 363 bis y 363 ter, debe producir daño o beneficio económico o transferencia patrimonial.

El perito informático dirá sobre los aspectos técnicos, sin embargo no podrá concluir sobre el daño o beneficio económico. No solo se debe tomar en cuenta delitos donde las cosas son obvias sino pensemos en aspectos donde el daño no es tan visible y pueden darse figuras como el lucro cesante o daño emergente.

Para definir la selección del perito se debe tomar en cuenta primero el ordenamiento legal:

- NCPP Artículo 204º.- (Pericia)
- NCPP Artículo 205º.- (Peritos)

NCPP Artículo 204º.- (Pericia)

- Se ordenará una pericia cuando para descubrir o valorar un elemento de prueba sean necesarios conocimientos especializados en alguna ciencia, arte o técnica.

NCPP Artículo 205º.- (Peritos)

- Serán designados peritos quienes, según reglamentación estatal, acrediten idoneidad en la materia. Si la ciencia, técnica o arte no está reglamentada o si no es posible contar con un perito en el lugar del proceso, se designará a una persona de idoneidad manifiesta. Las reglas de este Título regirán para los traductores e intérpretes.

En Bolivia no tenemos definido los criterios para seleccionar un perito informático sin embargo se practica aplicar los siguientes:

- Profesional de licenciatura o ingeniería de sistemas.
- Colegiado en la Sociedad de Ingenieros o Colegios de Informáticos legalmente reconocidos.
- Especializado en temas de seguridad por cuanto es lo más cercano a los trabajos periciales como formación reconocida.
- Trayectoria profesional mínima de 5 años.

Dada la conformación de equipos en las partes querellante y querellado, se debe tomar en cuenta la figura del consultor técnico.

Las atribuciones de este último están definidas legalmente en el Art. 207 c.p.p.

Artículo 207º.- (Consultores Técnicos)

- El juez o tribunal, según las reglas aplicables a los peritos, podrá autorizar la intervención en el proceso de los consultores técnicos propuestos por las partes.El consultor técnico podrá presenciar la pericia y hacer observaciones durante su transcurso, sin emitir dictamen. En las audiencias podrán asesorar a las partes en los actos propios de su función, interrogar directamente a los peritos, traductores o intérpretes y concluir sobre la prueba pericial, siempre bajo la dirección de la parte a la que asisten. La Fiscalía nombrará a sus consultores técnicos directamente, sin necesidad de autorización judicial.

NCPP Artículo 209.- (Designación y alcances

- Las partes podrán proponer peritos, quienes serán designados por el fiscal durante la etapa preparatoria, siempre que no se trate de un anticipo jurisdiccional de prueba, o por el juez o tribunal en cualquier etapa del proceso. El número de peritos será determinado según la complejidad de las cuestiones por valorarse. El fiscal, juez o tribunal fijarán con precisión los temas de la pericia y el plazo para la presentación de los dictámenes. Las partes podrán proponer u objetar los temas de la pericia.

ACTA DE POSESIÓN

- Es importante el acta de juramento previo caso contrario podemos invalidar nuestro trabajo

LiveCDs Forenses (Tarea 1)

Para comenzar desde cero, una buena opción es conocer diferentes paquetes de herramientas de análisis forense que se distribuyen comercialmente, o bien de forma gratuita.

Hay que considerar que las soluciones que se ofrecen son muy similares en cuanto a posibilidades, de modo que utilizar una u otra opción dependerá casi del gusto de cada uno y de la facilidad con la que nos familiaricemos con cada herramienta. A continuación se relacionan diferentes opciones.

Forensic Toolkit

- FTK (Forensic Tool Kit) es un paquete de herramientas forenses muy utilizado por los profesionales. Se trata de una distribución comercial. Permite análisis de correo electrónico y de archivos comprimidos, opciones de búsqueda de archivos y restauración de datos, así como múltiples archivos y formados de adquisición.

DEFT

- DEFT (Digital Evidence & Forensic Toolkit) es una distribución Live CD basada en Linux Kernel 3 y DART (Digital Advanced Response Toolkit). Se trata de un proyecto italiano de gran éxito, por cierto, y que incluye las mejores herramientas forenses. Además de un número considerable de aplicaciones de Linux y scripts, DEFT también cuenta con la suite de DART que contiene aplicaciones de Windows.

HELIX

HELIX es otra famosa distribución Linux basada en Ubuntu para respuesta a incidentes y análisis forense. Está desarrollada por e-fense y, aunque sus versiones iniciales eran gratis, desde hace unos años se ofrece como un producto de pago. Dispone de una versión de evaluación por 30 días, ideal para probar el producto.

Hay que decir que muchas de las herramientas basadas en Live CDs se ejecutan directamente sobre el terminal, y en la mayoría de las distribuciones Linux que hemos probado el teclado no está configurado en español, lo que dificulta la escritura de parámetros, por ejemplo. Por ello, es conveniente cambiar la configuración del teclado.

Artefactos forenses

Principio de intercambio de Emond Locard:

> “Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto”,
>
> Los sistemas operativos cuentan con procesos o mecanismos de registro sobre toda actividad realizada por el sistema o el usuario, programas utilizados, accesos, conexiones, aplicaciones, descargas desde Internet, etc.

Estos elementos nombrados anteriormente son considerados como “artefactos”, agrupamos los artefactos de acuerdo a la actividad:

- Archivos Descargados
- Ejecución de programas
- Creación y Apertura de archivos
- Eliminación de archivos
- Locación física
- USB & Dispositivos
- Uso de Cuentas
- Uso de Navegadores

Tarea

-
- Prueba digital
- Evidencia digital
-