INFORMÁTICA FORENSE

A/C Estefanía Cantero, CISM

Estefania.Cantero@arnaldocastro.com.uy

ECSeguridad@gmail.com

Junio, 2007

Montevideo - Uruguay

ARNALDO C. CASTRO S.A.

ISACA®

Serving IT Governance Professionals

Agenda

- Porque informática forense?
- Definiciones y objetivos del área
- Incidentes de seguridad e ilícito informático
- Peritaje informático
  - Evidencia digital
  - Principios metodológicos
  - Cadena de custodia
  - Procedimientos
- Software y hardware forense
- Conclusiones y desafíos

Introducción

INFOBAE *profesional.com*

HOME | ABOGADOS | CONTADORES | ECONOMIA | FINANZAS | COMEX | TECNOLOGIA | MARKETING | M

El FBI descubre fraude accionario online en hoteles y cibercafés

Cuando un inversionista utiliza una computadora pública para revisar sus acciones o hacer alguna transacción, sus datos son capturad

Decenas de millones de dóla en un fraude de rápido cre cibercafés, dijeron funcionar por sus siglas en inglés.

20minutos.es | Tecnología

Jueves, 17/05/07. **Actualizado hace 1 minuto**

El

Portada | Tu ciudad | Gente | Tele | Deportes | Blogs/Opin

culpa de Lara Croft | día de internet | juego mat

Enviar | Imprimir

Artículo 6 de 8 en Tecnología « Anterior

PUBLICIDAD

ELECCIONES 27M | Comunidades y ayuntamiento

El acusado del mayor ataque informático militar de la historia será extraditado a EEUU

EFE. 03.04.2007 - 12:08h

- Accedió a ordenadores de la NASA, el Ejército, la Marina, el Departamento de Defensa y la Fuerza Aérea de EE UU.
- Es el mayor asalto a un sistema informático militar de todos los tiempos.

EL PAIS digital

INICIO CONTACTO MI PERFIL PUBLICIDAD EL PAIS MOVIL EL PAIS LEIDO FAVORITOS PAG INICIO

INFORMACION | OPINION | DEPORTES | SUPLEMENTOS | SERVICIOS | OCIO | CANA

CONTROL DE ACCESO ◄ volver

MP3

Música y tecnología

Una abuela condenada por bajar música. La justicia francesa exigió a Marie-Thérèse Olivet, una mujer de 66 año el pago de 650 dólares por descargar 2899 canciones de Internet. "No tengo la sensación de tener ante mí a una delincuente y por eso creo que la justicia optó por la mesura", dijo el abogado de la defensa, Jean Louis Pujol, respecto a la sentencia que terminó siendo una pena simbólica como había solicitado el fiscal hace un mes. Olivet salió llorando del juzgado y se recluyó en su casa en Albias, un pueblo de 3 mil habitantes cerca de Montauban al suroeste del país galo. Hasta allí llegó la policía en el 2005 con una orden judicial para allanar su

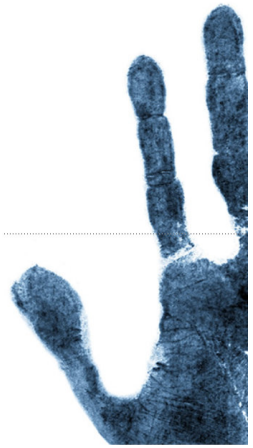
ISACA

Porque informática forense?

- La actividad informática se ha vuelto fundamental en la vida de las organizaciones y de las personas
  - Valor de la información
  - Conectividad

Ciencia forense

- Por definición es la aplicación de prácticas científicas dentro del proceso legal



- Significado: determinar el valor probatorio de una escena de crimen y su evidencia relacionada

Informática forense

- Definición
  - Serie de técnicas y procedimientos metodológicos para capturar evidencia de equipamientos computacionales y dispositivos digitales que pueden presentarse como evidencia en una prueba, de forma coherente y significante

- Para que?
  - Procesamiento judicial
  - Investigación en ámbito organizacional

Incidentes de seguridad

- Acceso no autorizado
- Pérdida de
  - Confidencialidad (planes de negocio, información personal)
  - Integridad (cambios de bases de datos, fraude)
  - Disponibilidad (denegación de servicio, daño a los sistemas)
- Uso indebido (de sistemas, de datos o en contra de las políticas establecidas)

Ilícito informático

Universidad del Martes/06-Mar-2007 (3) | Hoy

Ingresar

Ley de Propiedad Intelectual espera disminuir avance de la piratería

Los estudiantes de Derecho que aprobaban sin tener que rendir

En la Universidad Nacional de Tucumán se detectó la adulteración de notas.
Hay once empleados sumariados e interviene la Justicia.

PROPIEDAD INTELECTUAL | PROTECCION DE DATOS PERSONALES | DERECHO LABORAL

Phishing: Un peligro para la banca on-line

27/11/2006

HFD> Derecho Informático - Internet > Jurisprudencia Argentina

FALLO SOBRE USO INDEBIDO DEL CORREO ELECTRÓNICO EN EL LUGAR DEL TRABAJO DICTADO POR LA SALA VII DE LA CÁMARA LABORAL DE LA CIUDAD DE BUENOS AIRES

HOME | ABOGADOS | CONTADORES | ECONOMIA | FINANZAS | COMEX | TECNOLOGIA | MARKETING

Extorsiones informáticas, una nueva modalidad delictiva

Hackers a sueldo, la nueva moda para espionaje entre empresas

Funcionario de USA implicado en caso de Pedofilia

El subsecretario de prensa del Departamento de Seguridad Interior de Estados Unidos, Brian Doyle, fue

Ilícito informático

- Actividades ilegales que involucran el uso de un computador
  - Como objetivo del ilícito
  - Como medio para llevar a cabo el ilícito
  - Evidencia indirecta de otros ilícitos o litigios (juzgado de familia)

- En Uruguay no está definido el delito informático

Experiencia en Uruguay

- ISACA Montevideo firmó un convenio con el Instituto de Derecho Informático (IDI) de la Universidad de la República
  - Formación de un grupo de Peritaje Informático
  - Elaboración de un marco regulador de la actuación y metodología utilizada por el perito informático
  - El resultado del grupo será avalado por jueces, fiscales, abogados, peritos, auditores, investigadores

Grupo de trabajo IDI/ISACA

- Concepto de prueba
  - Para el derecho la prueba es “el conjunto de reglas que preparan la admisibilidad, la producción, la carga y la fuerza probatoria de los diferentes medios de prueba que pueden utilizarse para da al Juez la convicción sobre los hechos concernientes al proceso”
  - La actividad probatoria puede desarrollarse dentro del proceso o antes, refiriéndose entonces a la prueba preconstituida o adelantada.
- Medios probatorios
  - Son los modos en que se materializa la actividad probatoria
  - Entre los distintos medios probatorios está la prueba pericial

Grupo de trabajo IDI/ISACA (cont)

- Prueba pericial
  - Se realiza cuando haya necesidad o conveniencia de que determinados hechos o circunstancias sean estudiados desde la perspectiva de un conocimiento específico.
  - Actividad desarrollada por terceros ajenos al proceso que tiene como fin emitir una declaración valorativa de ciertos hechos para ayudar a crear el convencimiento judicial
  - La prueba pericial puede ser usada tanto en procesos civiles como en procesos penales

Peritaje informático

- Investigación orientada a la obtención de una prueba de aplicación en un asunto **judicial** para que sirva a un Juez

- La disciplina combina técnicas científicas y elementos legales para
  - Extraer
  - Preservar
  - Analizar
  - Presentar

Rol

- Cual es el rol de la informática forense en la actividad legal?
  - Identificación de una actividad ilegal
  - Obtención de la evidencia
  - Construcción/mantenimiento de la cadena de custodia
  - Preservación de la evidencia
  - Investigación de la evidencia
  - Presentación de los resultados al decisor

Requisitos

- Metodología y procedimientos
- Recursos humanos
  - Habilidad y capacitación de los técnicos
  - Credibilidad y confianza (Códigos de ética profesional)
  - Entrenamiento en la metodología
- Situación actual: distintos grados de madurez en la formalización del tratamiento de la evidencia digital

Fuentes / Registros

- Pueden ser tan diversas como elementos digitales existen
  - Conexiones a la red y al PC
  - Análisis de archivos (contenido, propiedad, etc.)
  - Recuperación de archivos eliminados
  - Cintas de respaldo
  - Agendas
  - Registro de llamadas telefónicas
  - Trazas de auditoria, registros de log

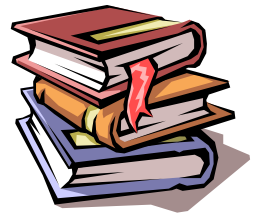
Evidencia digital

- Información almacenada o trasmitida en forma digital que puede ser utilizada como prueba
- Características críticas
  - Frágil
  - Volátil
- Ventajas
  - Repetible
  - Recuperable

Dificultades

- Falta de cuidado en la conservación de los equipos
- Alteración de la evidencia por falta de protección
- Se llega tarde a levantar la evidencia (se pierden registros o se sobreescriben)
- Falta de recursos humanos y materiales adecuados

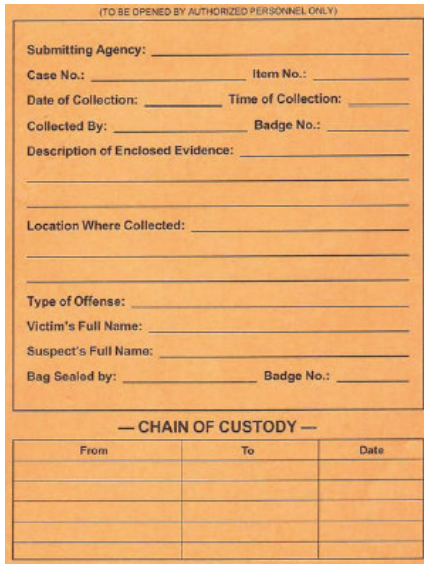
Principios metodológicos



- El perito debe ser objetivo y observar los códigos de ética profesional
- Conservar la autenticidad e integridad de la evidencia
  - Obtener la evidencia sin corrupción
  - Minimizar el trabajo sobre la evidencia original
  - Documentar cualquier cambio en la evidencia (cadena de custodia)
  - Autenticar la evidencia

Cadena de custodia

- Documenta el proceso completo de las evidencias durante la vida del caso
  - Quien y donde se recogió la evidencia
  - Como se almacenó
  - Quien la procesó, etc.
- Asegura:
  - Identificación
  - Continuidad de la posesión
  - Prueba de integridad



(TO BE OPENED BY AUTHORIZED PERSONNEL ONLY)

Submitting Agency: _____

Case No.: _____ Item No.: _____

Date of Collection: _____ Time of Collection: _____

Collected By: _____ Badge No.: _____

Description of Enclosed Evidence: _____

Location Where Collected: _____

Type of Offense: _____

Victim's Full Name: _____

Suspect's Full Name: _____

Bag Sealed by: _____ Badge No.: _____

— CHAIN OF CUSTODY —

From	To	Date

Peritaje - Preparación

- Aceptación de la pericia
  - Entender y evaluar la solicitud
  - Determinar las habilidades requeridas
- Preparación
  - Diagnosticar y entender el entorno (entrevistas)
  - Identificar sitios, respaldos
  - Identificar la arquitectura tecnológica (selección de herramientas)
  - Preparación de formularios
  - Materiales para identificación y traslado

Primer contacto

- Separar a las personas de las máquinas
- Notificar (testigos)
- Anotar nombres
- Documentar fechas y horas (de arribo, de la máquina)
- Clasificar la evidencia según su grado de volatilidad
- Clasificar la evidencia en orden de relevancia
- Considerar la evidencia física (papeles, notas, etc.)
- Obtener claves (entrevistas)
- Documentar hardware y software, fotografiar
- Iniciar cadena de custodia

Preservación de evidencia volátil

- Evidencia volátil
  - Se pierde al apagar la máquina (usuarios conectados, procesos en ejecución, estado de la memoria, etc.)
  - Información del disco (fechas de acceso a archivos, archivos temporales)
- En lo posible no apagar la máquina y recoger inmediatamente la evidencia volátil sin alterar la escena
- Usar el mínimo de memoria posible para no sobrescribir
- Aislar la máquina de la red para evitar alteraciones
- Guardar la información en otro dispositivo
  - Pendrive, otro equipo seguro, etc.

Preservación de evidencia persistente

- Apagar sin correr secuencia de bajada
- Documentar conexiones
- Identificar y precintar
- Utilizar material adecuado para el transporte (interferencia electromagnética, humedad)
- Guardar en lugar seguro y limpio
- Verificar secuencia de booteo
- Utilizar software forense
  - Bootear con un sistema propio
  - Autentificar (hash)
  - Copia bit-a-bit (2 copias para trabajo)

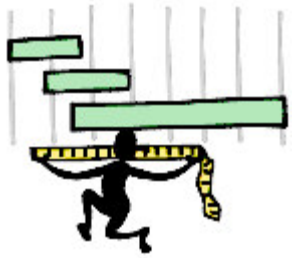
Extracción / Inspección

- Objetivo: identificar y localizar evidencia potencial
- Documentación de datos básicos
  - Sistema operativo, configuración de red, aplicaciones, trabajos agendados, usuarios del sistema, etc.
- Extraer datos protegidos, cifrados o comprimidos
- Extraer logs y trazas de auditoria
- Extraer datos a nivel del sistema de archivos
  - Fechas, permisos, caminos, papelera de reciclaje, archivos temporales, información del autor (Office)
- Extraer datos a nivel físico
  - Archivos borrados, búsqueda hexadecimal, tabla de particiones, espacio no asignado, espacio reservado
- Descartar archivos irrelevantes (bases de hash)

Análisis / Interpretación

- Objetivo: determinar el significado de los datos examinados y establecer la conclusión de la pericia
- Generación de hipótesis y armado de la prueba

- Análisis temporal
  - identificación de momento y secuencia de los eventos
- Análisis funcional
  - relacionar los eventos



Presentación de resultados

- Admisibilidad
  - Autenticidad (la evidencia debe estar relacionada con el caso y no alterada)
  - Confiabilidad (forma de registro comprobable)
  - Suficiencia (redundancia y correlación de eventos)
  - Conformidad con la legislación vigente
- Criterio de razonabilidad
- Presentar la documentación en un leguaje entendible para los destinatarios

Metodología y estándares

- Buenas prácticas en gestión de tecnología: ISO 17799:2005 – 13.2.3 “Recolección de evidencias”
  - Reglas para las evidencias
    - Validez, admisibilidad de la evidencia
    - Calidad y completitud de la evidencia
  - “ Cuando se detecte un incidente, al principio no es obvio que se convierta en una posible actuación ante el juzgado. Sin embargo, existe el peligro de que las pruebas se destruyan accidentalmente antes de que se confirme la seriedad del incidente”

Metodologías y estándares

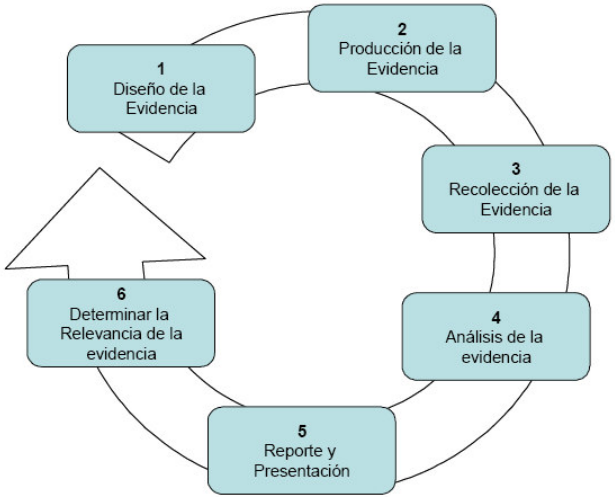
- Dentro de las Auditorias Internas se está definiendo formalmente el proceso de Auditoria Forense:
  - “Realizar auditoria forense, asegurando la adecuada identificación, recolección, preservación y manipulación de elementos informáticos que serán utilizados como evidencia digital en una investigación”

Metodologías y estándares

- HB171:2003 “Handbook guidelines for the management of IT evidence”
  - Proveer una guía para la gestión de los registros electrónicos que pueden ser usados en procedimientos judiciales o administrativos o cuando se sospecha de actividad ilegal
  - Provee un ciclo de vida para la administración de la evidencia digital

Gestión de la evidencia digital

- Clasificar la información (establecer relevancia de la evidencia)
- Determinar tiempos de retención
- Diseñar los registros de auditoría y sincronizar
- Seguridad de los registros (autenticidad, integridad)



Readiness

- Maximizar la habilidad de la organización de utilizar evidencia digital minimizando los costos de investigación
  - Gestión de incidentes
  - Auditoria y trazabilidad
  - Almacenamiento y manejo de evidencia potencial
  - Soluciones tecnológicas
    - Logs: que y como se logea
    - Herramientas de análisis y monitoreo de controles de seguridad
    - IDS, IPS, Antivirus, etc.

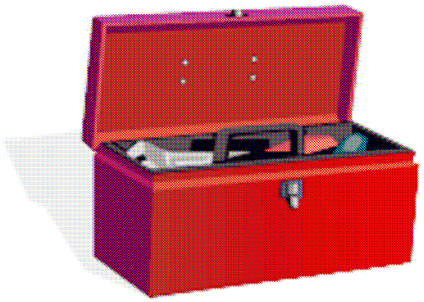
Software forense

- Kits
  - EnCase, FTK, Helix, Sleuth Kit, Knopix STD
- Herramientas
  - Recuperación de passwords
  - Herramientas de esteganografía
  - Imágenes y bloqueadores de discos
  - Indizadores/buscadores de palabras en binario
  - Recuperación de archivos borrados desde cualquier tipo de almacenamiento externo
  - Recuperación de datos de navegación y correo

Herramientas de software

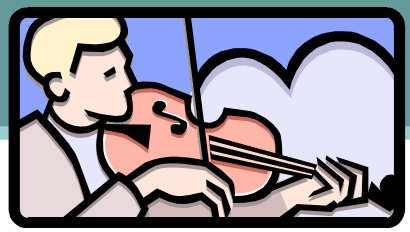
- Herramientas para redes
  - Captura de tráfico hasta capa de aplicación
  - Aplicaciones asociadas a puertos abiertos
  - Listados de puertos abiertos
  - Vista de arquitectura
- Herramientas ANTIFORENSE
  - Borradores de disco
  - Herramientas de booteo
  - Ocultadores de archivos
  - Eliminadores de evidencia (trazas de actividad en distintas aplicaciones, limpiadores de log, etc.)
  - Herramientas de esteganografía

Hardware forense



- Password crackers
- Bloqueadores de disco
- Copiadores de disco
- Laptops, laboratorio móvil
- Bolsas y etiquetas para sellado y transporte

Problemas



- La computación forense todavía está en desarrollo
- Falta de entrenamiento apropiado y designación profesional
- No existe estandarización de las herramientas

La informática forense todavía es mas un “arte” que una “ciencia”

Otros problemas

- Falta de conocimiento o experiencia de los técnicos
- Uso de software poco conocido o antiguo
- Malas prácticas en el tratamiento de la evidencia
- Falta de recursos materiales
- Subestimar el alcance del incidente
- Existencia de software anti-forense
- Falta de objetividad
- Fallas en la documentación o alteración de la cadena de custodia
- Fallas en el informe

"Estar preparados"

- Mantener trazas de uso de aplicaciones, sistemas, red, etc.
- Revisar las trazas
- Aplicar principios de seguridad (equipamiento y procedimientos)
- Mantener los relojes sincronizados
- Capacitación
- Campañas de sensibilización
- Conocer el entorno y el comportamiento normal
- Auditar

Desafíos

- Establecer un marco regulatorio y procedimientos para la pericia informática
- Estándares de ética y privacidad
- Profundizar en el conocimiento de los aspectos legales
- Formación en peritaje informático

Muchas gracias

A/C Estefanía Cantero, CISM

Estefania.Cantero@arnaldocastro.com.uy

ECSeguridad@gmail.com

Montevideo - Uruguay

ARNALDO C. CASTRO S.A.

ISACA
Serving IT Governance Professionals