ANÁLISIS FORENSES

INTRODUCCIÓN

Ciencia Forense

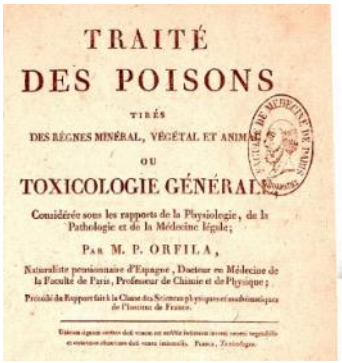
Aplicación de las ciencias físicas a la ley en la búsqueda de la verdad, en materia de comportamiento civil, penal y social a fin de que la injusticia no se haga a cualquier miembro de la sociedad

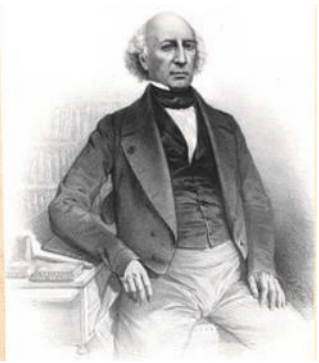
Handbook of Forensic Pathology College of American Pathologist 1990

Historia

- **Mathieu Orfila** (1787-1853): Traité des Poisons – Toxicología

- **Alphonse Bertillon** (1853-1914): Policía y científico interesado en la antropología.
  - Metodología para la obtención de evidencias (testigos métricos) y no alteración de la escena

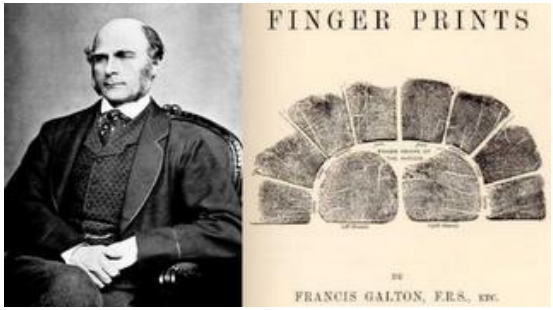

TRAITÉ
DES POISONS
TIRÉS
DES RÈGNES MINÉRAL, VÉGÉTAL ET ANIMAL
OU
TOXICOLOGIE GÉNÉRALE
Considérée sous les rapports de la Physiologie, de la Pathologie et de la Médecine légale;
PAR M. P. ORFILA,
Naturaliste pensionnaire d'Espagne, Docteur en Médecine de la Faculté de Paris, Professeur de Chimie et de Physique;



Historia

- **Francis Galton** (1822 -1911): Científico defensor de la eugenesia. Individualización de huellas digitales. Libro Finger prints

- **Hans Gross** (1847-1915): Juez y profesor austriaco. Acuño el termino criminalística referido al análisis sistemático de las huellas dejadas por el culpable



Historia

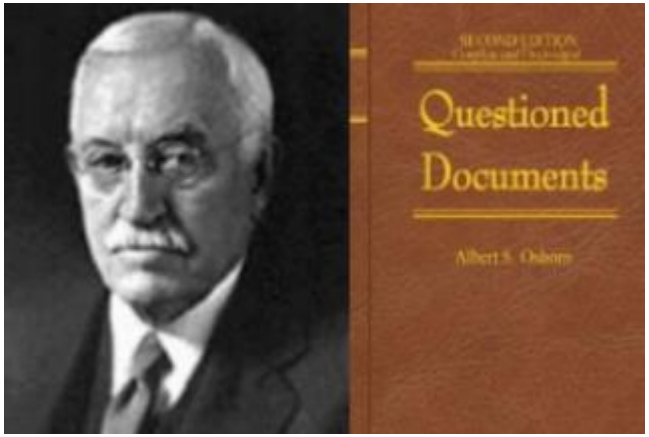
- **Edmon Locard** (1877 -1966): criminalista francés. Primer laboratorio forense en Lyon.
  - **Principio de Locard**: **Todo lo que entra en contacto deja un rastro**

- **Calvin Goddard** (1891-1955): Coronel e investigador. Desarrolló la balística.

Historia

- **Albert Osborn:** (1858-1946): el padre del peritaje caligráfico y examen de documentos.

- **J. Edgar Hoover** (1895 -1972): Fundo el FBI. En 1932 estableció el primer laboratorio criminal.



http://www.forensicdna.com/Timeline020702.pdf

Informática Forense

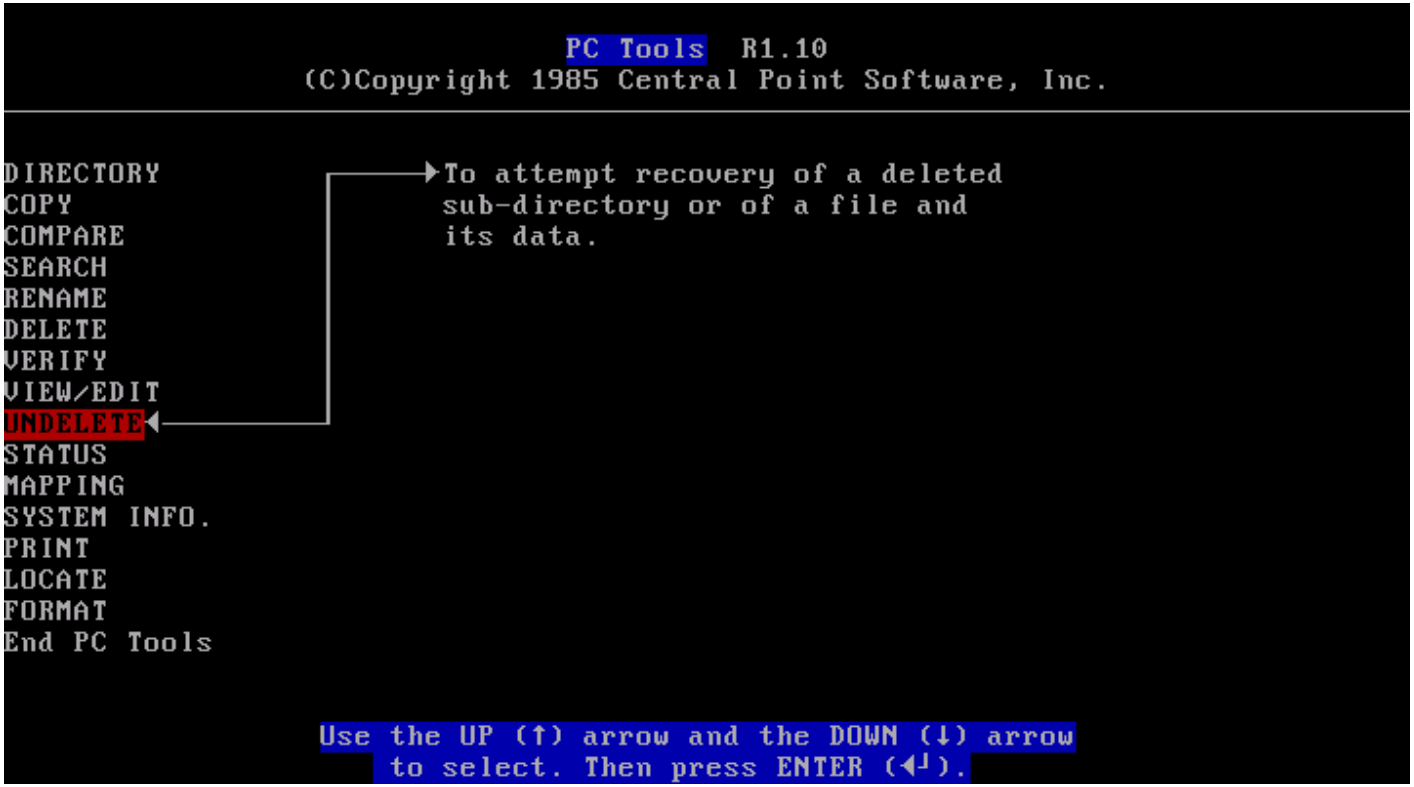
La aplicación de técnicas científicas y analíticas especializadas a **infraestructura tecnológica** que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Wikipedia

Informática forense - Historia

- 1981 - copy2pc de Central Point Software (Pc Tools)
- 1982 – UnErase: Norton Utilities 1.0
- 1984 – FBI Computer Analysis and Response Team (**CART**)
- 1987 – High Tech Crime Investigation Association (**HTCIA**)
- 1987 – Access Data
- 1988 - International Association of Computer Investigative Specialists – **IACIS**

Pc Tools


PC Tools R1.10
(C)Copyright 1985 Central Point Software, Inc.
DIRECTORY
COPY
COMPARE
SEARCH
RENAME
DELETE
VERIFY
VIEW/EDIT
UNDELETE
STATUS
MAPPING
SYSTEM INFO.
PRINT
LOCATE
FORMAT
End PC Tools
To attempt recovery of a deleted sub-directory or of a file and its data.
Use the UP (↑) arrow and the DOWN (↓) arrow to select. Then press ENTER (↵).

Informática forense - Historia

- 1988 - Seized Computer Evidence Recovery Specialists - **SCERS**
- 1990 - **Xtree** Gold (undelete)
- 1991 – **Libro** Guide to Data Recovery (Scott Mueller)
- 1992 – ExpertWitness de ASR Data
- 1995 - International Organization on Computer Evidence – **IOCE**
- 1996 – **iLook** de Perlustro v2
- 1997 – Scientific Working Group of Digital Evidence (**SWGDE**)
- 1998 – Interpol - Forensic Science Symposium
- 2001 – Digital Forensic Research Workshop (**DFRWS**)

Descripción

¿Por que?

Responde a la necesidad de **aclarar** un **incidente** relacionado con la **seguridad informática**. Puede tener distintos origenes:

- Humano.
- Funcional.

¿Como?

Analizando minuciosamente cualquier dato generado, modificado o eliminado a raíz del incidente.

Descripción

¿Cuando?

Con la **mayor rapidez posible** para evitar que las evidencias sean contaminadas.

¿Donde?

En **todos** los elementos digitales que **almacenen información** y estén relacionados con el incidente.

El criterio de *Daubert*

Se basa en cuatro factores utilizados para evaluar las evidencias científicas:

1. Pruebas realizadas
2. Revisiones cruzadas (*peer review*)
3. Tasa de error (*error rate*) de las pruebas
4. Aceptación por la comunidad científica

Tipos de análisis forenses

- Análisis de sistemas
  - Estaciones de trabajo
  - Servidores
- Análisis de memoria
- Dispositivos móviles
- Forenses de red

Motivos para hacer un análisis forense

- Legal
  - Cumplimiento regulatorio
  - Proceso civil o criminal
- Negocio
  - Seguridad de la información y garantías
  - Daños financieros
- Administrativo
  - Violaciones de políticas

Cibercrimen

Cualquier acto que implica un ordenador, un sistema o una aplicación.

- Robo de propiedad intelectual
- Fraude financiero
- Penetración de sistemas
- Denegaciones de servicio
- Distribución de malware

Derecho Laboral

- Ejercicio de la facultad de dirección y control del empleador sobre el equipo informático proporcionado a los trabajadores para el desempeño de sus funciones (art. 20.3 Estatuto de los Trabajadores - ET)
- Abuso de confianza en el desempeño del trabajo (art. 54.2.d) ET)
- Transgresión de la buena fe contractual (art. 54.2.d) ET).
- Indisciplina o desobediencia en el trabajo (art. 54.2.a) ET)

Derecho Penal – 1/2

- Descubrimiento y revelación de secretos (arts. 278 - 280 Código Penal -CP)
- Delitos económicos/societarios (arts. 290-295 CP)
- Delitos contra la propiedad intelectual e industrial - Espionaje industrial (art. 200 y 273 CP).
- Vulneración de la intimidad, lectura de correos electrónicos, interceptación de comunicaciones, protección de datos personales (art. 197 CP).
- Amenazas (.art. 169 CP) y Delitos contra el honor (calumnias o injurias – arts. 205 y 208 CP)
- De las defraudaciones (estafas – art. 248 CP).

Derecho Penal – 2/2

- Revelación de Secretos e Informaciones relativas a la Defensa Nacional (arts. 598 y 599 CP)
- Análisis de plagio en programas informáticos (art. 270 CP).
- Difusión, revelación o cesión a terceros de imágenes captadas sin consentimiento o mediante otros medios ilícitos (intercambio P2P) (art. 197.4 CP).

Derecho mercantil - civil

- Competencia desleal y abuso de confianza.
- Análisis de plagio en programas informáticos.
- Cumplimiento de obligaciones y contratos informáticos.
- Verificar y comprobar implantación informática contratada.
- Publicidad engañosa o sin consentimiento por medios electrónicos.
- Venta de cosa ajena vía Internet.

Investigaciones privadas

- Realizadas de forma privada o por una compañía.
- Denuncias frecuentes:
  - Robo de propiedad intelectual
  - Usurpación de correos
  - Abuso de Internet
  - Espionaje
  - Sabotaje
- Establecer políticas de seguridad:
  - Uso de equipo informático, móviles, etc
  - Avisos (banners)

Investigaciones públicas

- Realizadas por cuerpos de seguridad: GDT / BIT
- Previa denuncia
- Casos comunes:
  - Pedofília y Cibercrimen
- Investigación judicial:
  - Orden de registro
  - Informe técnico

Tareas de un analista forense

1. Identificar el crimen
2. Obtener evidencias
3. Crear la cadena de custodia
4. Analizar las evidencias
5. Presentar las evidencias
6. Testificar

Evidencia

- La evidencia es lo que prueba que un hecho ocurrió o no
- Existen tres tipos de pruebas
  - Testimonio de un testigo
  - Evidencia física
  - Evidencia electrónica
- Cibercrimen y **crimen tradicional** pueden dejar pruebas electrónicas.

Caso: Bobbie Jo Stinnett

- Mujer embarazada es asesinada y su feto robado
- La mujer había publicado su estado en un foro en Internet
- La asesina se hizo pasar por una compradora de mascotas

Tipos de evidencia

- Prueba de cargo (inculpatoria) que apoya una teoría dada
- Prueba de descargo (exculpatoria) que contradice una teoría dada

- Evidencia admisible, permitidas en un juicio
- Pruebas inadmisibles, no permitidas en juicio
- Pruebas viciadas, obtenidas ilegalmente (por ej. sin orden judicial)

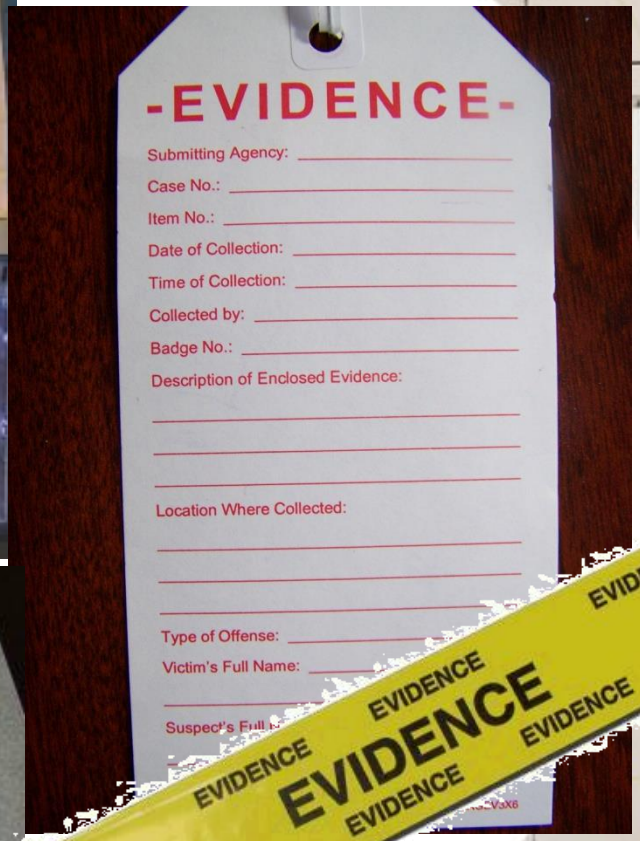
Tipos de evidencia - II

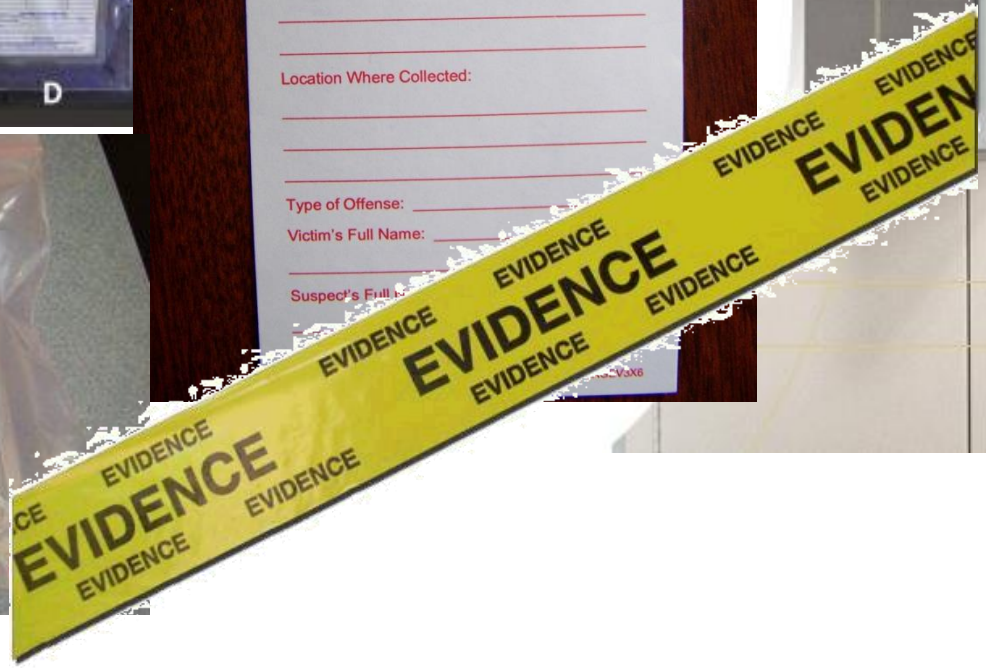
- Evidencia circunstancial: no prueba directamente la existencia o comisión de un hecho
- Testimonio indirecto (prueba basada en rumores, referencias, etc)

Cadena de custodia

- Objetivo: Identificación y autenticación
  - La evidencia es la que se buscaba
  - No ha sido alterada desde su obtención
- Función: posesión y control
  - Documentar la obtención, transporte y transferencia.
  - Muestra quien es el responsable
- Se basa en documentación solida
  - Características únicas (ej. número de serie)

Obtención de evidencia





Seguridad de la evidencia

- Uso de bolsas de evidencias
- Usar sistemas de manipulación:
  - Bolsas antiestáticas
  - Alfombrillas antiestáticas
- Contenedores con candados
- Uso de precinto de evidencia
  - Unidades de CD, Disquetera
  - Cordón de electricidad
- Escribir en el precinto para asegurar que no ha sido abierto
- Control de temperatura y humedad.

Consecuencias de la ruptura

- Especular de lo que realmente ha ocurrido
  - El juez decide si permite la evidencia
  - Las dudas restan importancia a la evidencia

- Rupturas importantes en la cadena
  - Error en la identificación
  - Contaminación
  - Perdida de evidencias

Errores comunes

- Confiscación no autorizada
- Destrucción de evidencias
- Errores en fechas
  - Hora del sistema
  - Zona horaria
- Actividades ilegales
  - Software sin licencia

RFC 3227 recolección y manejo de evidencias

- Principios para la recolección de evidencias
- Orden de volatilidad
- Acciones que deben ser evitadas
- Consideraciones relativas a la privacidad de los datos

RFC 3227 recolección y manejo de evidencias - II

- Consideraciones legales
- Procedimientos de recolección
- Transparencia
- Cadena de custodia
- Metodologías de almacenamiento de evidencias

CSIRT

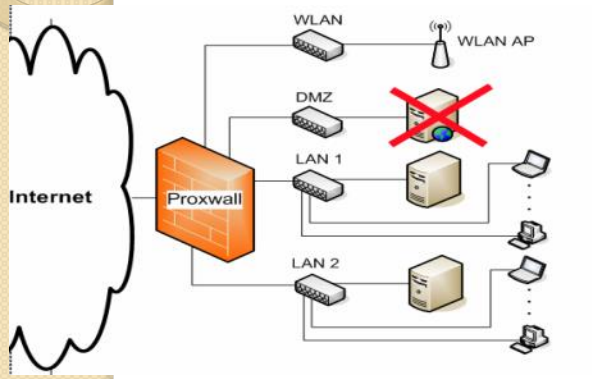
¿Qué es un CSIRT?

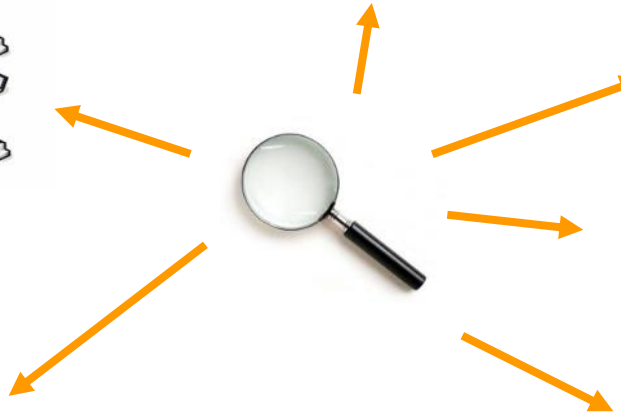
- Equipo de profesionales expertos.
- Detectan incidentes en fases previas, generando contramedidas para evitar futuras repeticiones.
- El CSIRT protege y asegura la información crítica de una organización: datos, hardware y políticas críticas del negocio.
- Forma en concienciación de seguridad, detección de intrusos y tests de intrusión.
- Incrementa la seguridad general de la organización
- Disminuye el tiempo de respuesta en un incidente

Ayuda en la toma de decisiones

- Determina si los datos sensibles han sido expuestos.
  - Diferencia entre tener que publicar o no
  - Notificar a tiempo reduce la responsabilidad
- Desarrollo de la estrategia futura
  - Presupuesto y respuesta ante incidentes
  - Revisión de políticas
- Resolución de conflictos
  - Conflictos civiles y penales
  - Gestión de recursos humanos.

Objetivos de un CSIRT






```
using( SqlConnection con = (acquire connection) ) {
  con.Open();
  using(SqlCommand cmd=new SqlCommand("SELECT * FROM
        users WHERE name = '" + uName + "'", con)){
  using( SqlDataReader rdr = cmd.ExecuteReader() ){
      ...
    }
  }
}
```

¿Qué es un incidente?

Cualquier evento adverso real o sospechado en relación con la seguridad de los sistemas o redes informáticos

Esto incluye:

- Acceso a sistemas remotos
- Spam
- Infección de códigos maliciosos
- Fuga de información
- etc

¿Cómo identificar un incidente? -indicio-

Algunos casos:

- Una alarma de un sistema de detección de intrusos
- Actividad inusual en la red o sistemas
- Intentos de acceso inválidos
- Incongruencias económicas
- Modificación de archivos

Tipos de incidente - I

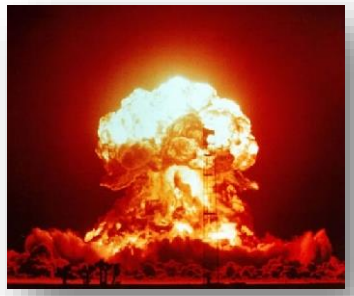
- Nivel bajo
  - Menos importantes
  - Un día para su solución
  - Ejemplos:
    - Perdida de contraseña
    - Sospecha de usuario compartido
    - Detección de análisis de puertos
    - Presencia vírica no propagada

Tipos de incidente - II

- Nivel medio
  - Debería gestionarse de 2 a 4 horas
  - Ejemplos:
    - Violación de acceso a un sistema
    - Almacenamiento y uso no autorizado de datos
    - Acceso ilegal a un edificio
    - Robo de un sistema o destrucción inferior a 100.00€

Tipos de incidente - III

- Nivel alto
  - Deben gestionarse inmediatamente
  - Ejemplos:
    - Denegación de servicio
    - Sistema al que se ha accedido
    - Virus con gran propagación
    - Destrucción o robo mayor de 100.00€
    - Cualquier aspecto que pueda ser un delito.



Gestión de incidentes

- Ayuda a identificar tendencias y patrones
- Se compone de tres funciones básicas: notificación, análisis y respuesta
- Se recomienda a los administradores de red para la recuperación, contención y prevención
- Se han de unir esfuerzos para aplicar la respuesta
- Ayuda a la dirección a entender el proceso de respuesta y hacer frente a amenazas no esperadas.

LABORATORIO

Laboratorio

- ISO/IEC 17025:19999 - General requirements for the competence of testing and calibration laboratories
- American Society of Crime Laboratory Directors (ASCLD) – certifica laboratorios

Requisitos

- Número de casos / sistemas necesarios
- Número de investigadores
- Espacio para salvaguardar evidencias
- Espacio para material de referencia
- Software
- Hardware
- Formación de especialistas
- Ergonómico

Laboratory Accreditation Board

Seguridad Física

- Protección ante inundaciones, incendios y otras catástrofes naturales
- Una sola puerta con registros de entrada y salida
- Armarios de almacenamiento seguros
- Registro de llaves, numeración, propietarios…
- Protección electricidad estática
- Contenedores de destrucción seguros
- Alimentación eléctrica (UPS)

Seguridad Lógica

- Sistemas forenses sin conectividad
- Red independiente
- Equipos hardware exclusivos
- Software actualizado
  - vulnerabilidades a productos de análisis forense (CVE-2007-4037)

Software

- Windows / Linux
- Software opensource y libre:
  - Autopsy / Sleuthkit / dcfldd / DEFT
- Software comercial:
  - EnCase
  - iLookPI
  - FTK
- Moviles
  - Parabean
  - Oxygen

Hardware

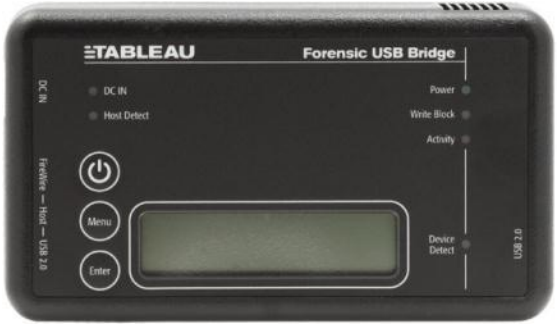
- Equipos especializados para el clonado

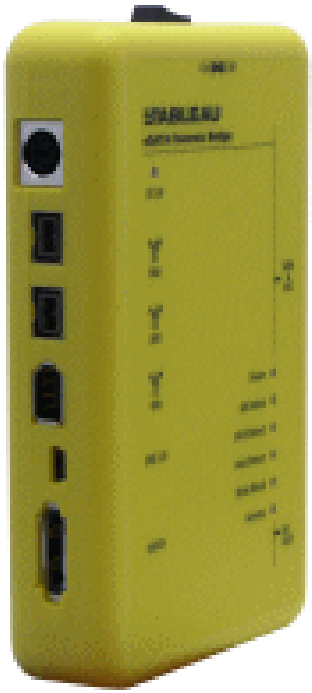
Hardware

- Equipos especializados para el análisis
- Equipos clónicos

Hardware

- Protectores de escritura (write blockers)



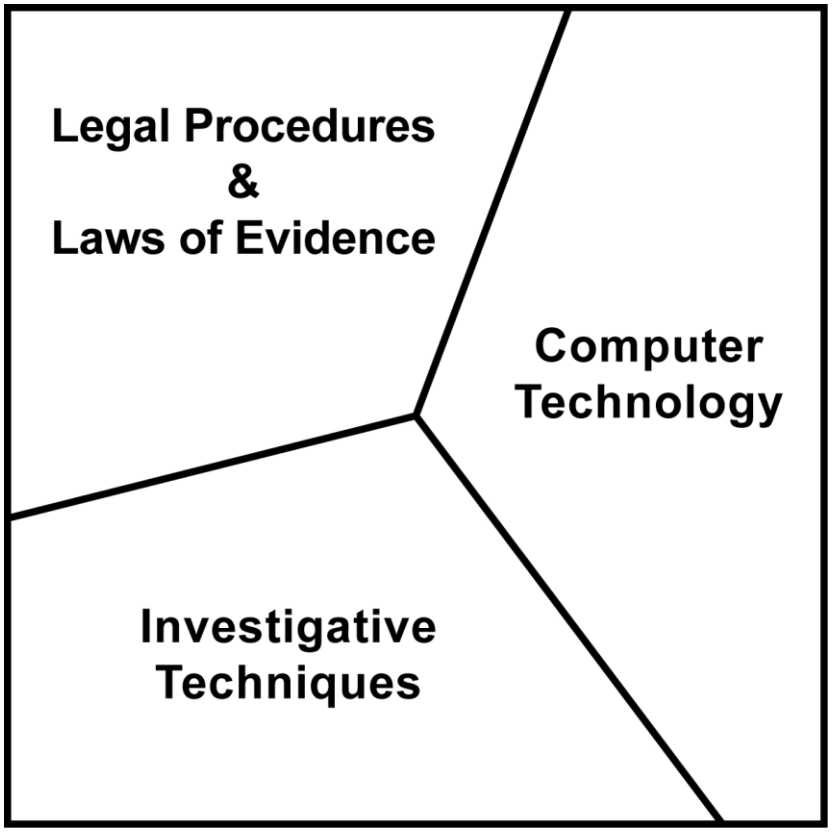


ANALISTA FORENSE

Conocimientos

- Metodología forense
- Altos conocimientos de sistemas operativos
- Sistemas de ficheros
- Formatos de documentos
- Técnicas de *hacking* y vulnerabilidades
- Criptografía

Áreas de conocimiento



Certificaciones

- SANS/GIAC
  - Certified Forensic Analyst - **GCFA**
  - Certified Incident Handler – **GCIH**
- ECCouncil
  - Computer Hacking Forensic Investigator – **CHFI**
- EnCase
  - EnCase Certified Examiner – **EnCE**
- Otras:
  - ISFCE – Certified Computer Examiner - **CCE**
  - HTCN– Certified Computer Forensic Technician -**CCFT**
  - ACFE - Certified Fraud Examiners - **CFE**

Código de ética

- Conducta profesional
  - Determina la credibilidad
  - Incluye ética, moral y normas de comportamiento
- Mantener la objetividad significa que debe formar y sostener opiniones sin prejuicios de sus casos
- Mantener la credibilidad de la investigación, manteniendo el caso confidencial
  - En entornos corporativos la confidencialidad es crítica
- En circunstancias especiales un caso corporativo se puede convertir en un delito penal tan serio como un asesinato.

Conducta profesional

- Mejorar tu conducta profesional con formación y entrenamiento
- Registrar todo los hallazgos en un cuaderno de bitácora.
- Atender a workshops y conferencias.
- Ser miembro activo de organizaciones especializadas.
- Conseguir alta reputación pública y privada, manteniendo la honestidad e integridad.

Artículo 335. Objeto y finalidad del dictamen de peritos. Juramento o promesa de actuar con objetividad.

1. Cuando sean necesarios conocimientos científicos, artísticos, técnicos o prácticos para valorar hechos o circunstancias relevantes en el asunto o adquirir certeza sobre ellos, las partes podrán aportar al proceso el dictamen de peritos que posean los conocimientos correspondientes o solicitar, en los casos previstos en esta ley, que se emita dictamen por perito designado por el tribunal.

2. **Al emitir el dictamen, todo perito deberá manifestar, bajo juramento o promesa de decir verdad**, que ha actuado y, en su caso, actuará con la mayor objetividad posible, tomando en consideración **tanto lo que pueda favorecer como lo que sea susceptible** de causar perjuicio a cualquiera de las partes, y que **conoce las sanciones penales en las que podría incurrir** si incumpliere su deber como perito.

Responsabilidad del Perito: Sanciones

- Cohecho (CP, Art. 419 al 422)
  - 1 a 6 años de prisión
  - Multa de hasta 3x el importe de la dádiva
  - Inhabilitación cargo público de 3 a 12 años.
- De las negociaciones y actividades prohibidas a los funcionarios públicos y de los abusos en el ejercicio de su función (CP, Art. 439)
  - 12 a 24 meses de multa
  - Inhabilitación cargo público de 3 a 6 años.
- Falso Testimonio (CP, Art 458 al 461)
  - 6 meses a 2 años de prisión
  - 3 a 12 meses de multa
  - Inhabilitación cargo público de 6 meses a 12 años.

Seguro de Responsabilidad Civil

- **CP, LIBRO I, TITULO V De la responsabilidad civil derivada de los delitos y faltas y de las costas procesales (Art. 109 al 129)**

- **Artículo 122.**

El que por título lucrativo hubiere participado de los efectos de un delito o falta, está obligado a la restitución de la cosa o al resarcimiento del daño hasta la cuantía de su participación.

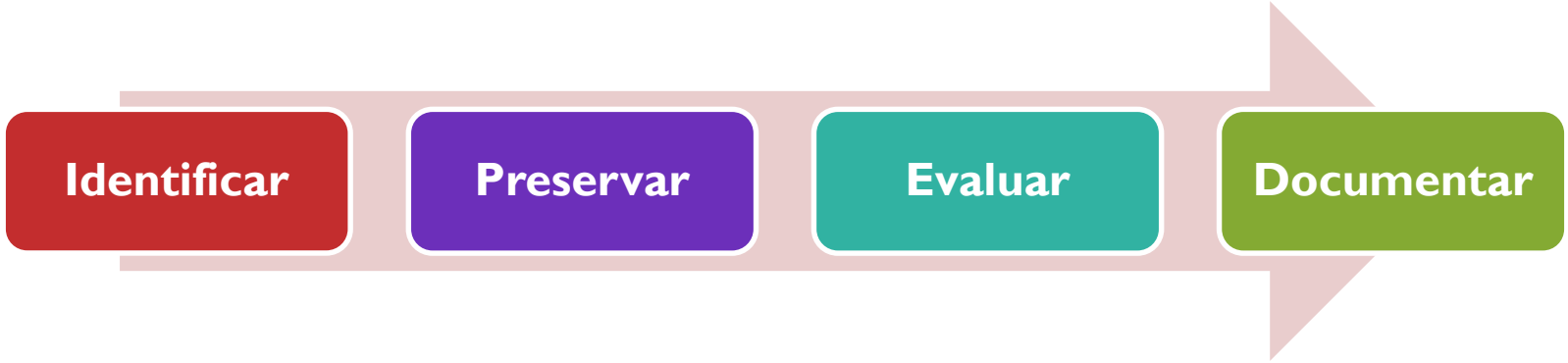
- **Artículo** 636. **(Artículo modificado por la Ley Orgánica 15/2003, de 25 de noviembre)**

Los que realizaren actividades careciendo de los seguros obligatorios de responsabilidad civil que se exigieran legalmente para el ejercicio de aquéllas serán castigados con la pena de multa de uno a dos meses.

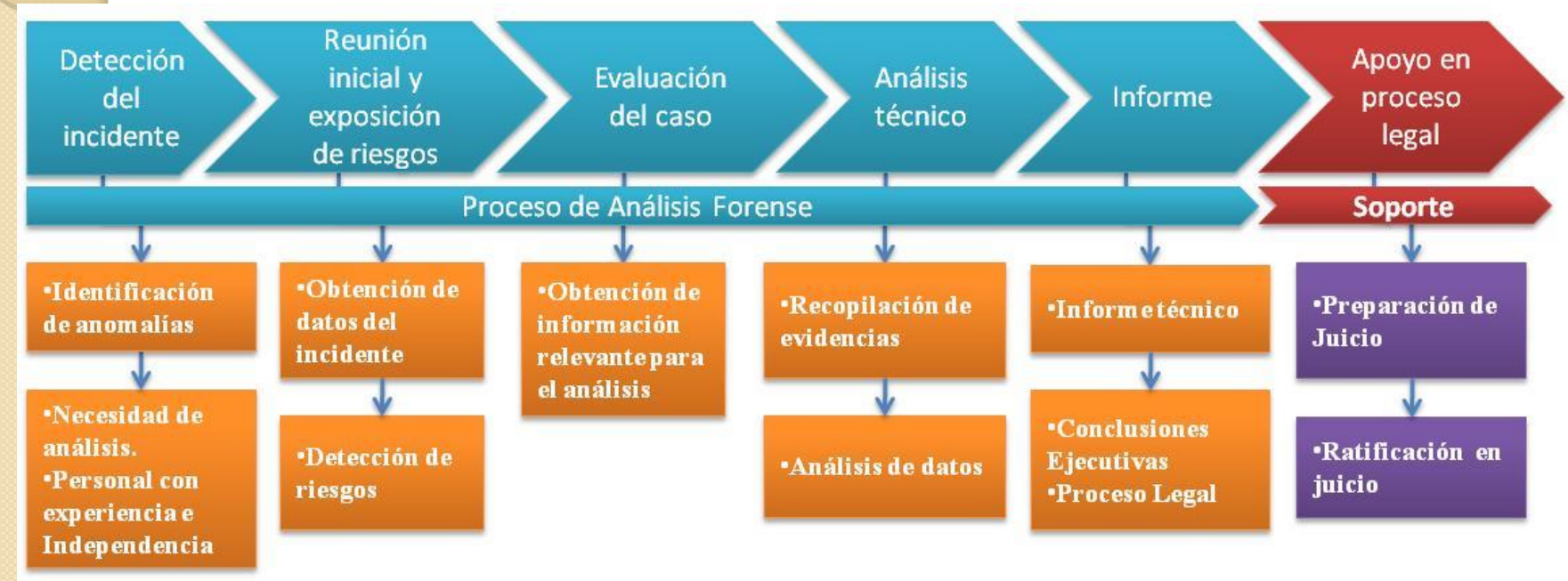
METODOLOGÍA

Metodología

"The computer forensic investigation process is a four step process, conducted after a crime was reported and a subpoena issued". *Holley, 2000*



Descripción de las fases



Reunión inicial

- Exposición del caso: Flujo lógico del proceso y otros datos (como se detectó, sospechas, plataforma tecnológica).
  - Componentes del equipo: (custodios, administradores, responsables) para cada elemento.
- Ámbito de conocimiento del incidente.

  - Régimen disciplinario interno, despido, negociaciones o vía judicial. (Requerimientos notariales)

Reunión inicial

- Exposición de riesgos técnicos y legales:
  - Los análisis sin salvaguardas pueden modificar la evidencia.
  - El inicio de un proceso legal en ocasiones puede ser detenido con posterioridad.
  - Tratamiento de evidencias electrónicas para no perder la validez legal de las mismas.

Evaluación del caso

- Existencia de mecanismos de **sincronización horaria**.
- **Logs** de DHCP, PDCs, Proxy, Firewal…
- Elementos de single **Sing-On**.
- Mecanismos de **registro de entrada y salida de personal.**
- **Accesos remotos** a la red (VPNs, Citrix, Webmail…)
- **Normativa interna** sobre uso de la plataforma informática.
- **Orden judicial** requerida para acceso a logs de proveedores de servicios de Internet.

Copia de discos

Tareas de análisis

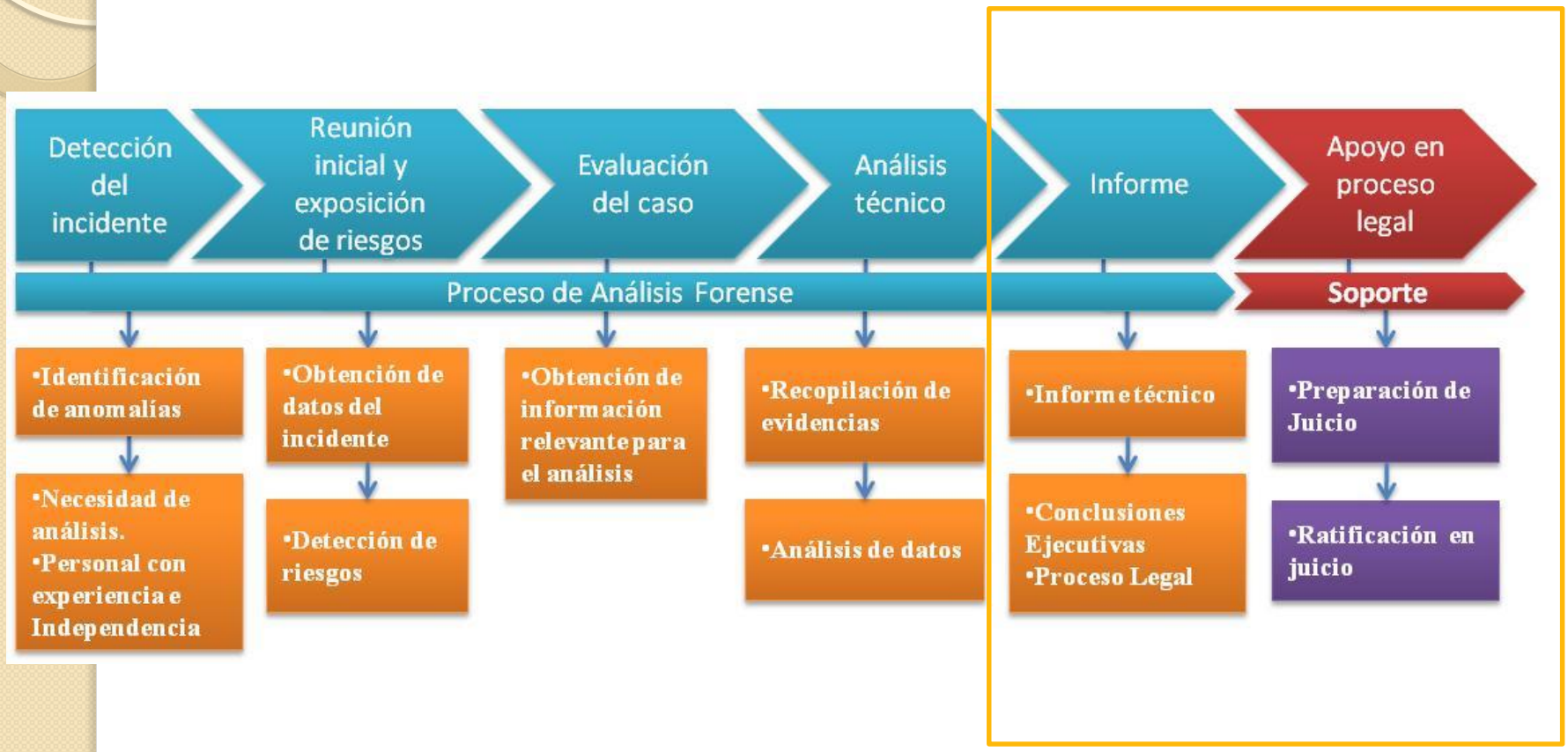
- Recuperación de datos borrados.
- Búsqueda de información en "metadatos“
- Depuración de aplicaciones troyanas en ejecución.
- Desensamblar binarios sospechosos.
- Romper archivos protegidos por contraseña
- Análisis de archivos temporales

Tareas de análisis

- Eventos en el sistema operativo
  - Login/Logoff
  - USBs conectados
- Identificación en línea de tiempo y correlación con otros eventos conocidos, de las acciones realizadas:
  - Aplicaciones instaladas y ejecutadas
  - Documentos modificados.
  - Cabeceras de correos enviados o recibidos y “timestamps” en servidores.
  - Creación y eliminación de cuentas de usuario.

DOCUMENTACIÓN

Descripción de las fases



Redacción de Dictamen (I)

Único resultado visible y perdurable

- PREGUNTA:
  - ¿Hay evidencias suficientes?
- EVIDENCIAS → Demostrables
  - Precio de mercado
  - Versión de SW instalada
- OPINIONES
  - Valoración de desarrollo a medida
  - Calidad del análisis funcional

Redacción de Dictamen (II)

Es importante incluir en el dictamen:

- Datos y Perfil del Perito
- Objeto, Antecedentes
  - Expediente Judicial, ...
- Período Temporal
  - Accesos / cambios …
- Fuentes de Información
- Criterios / Estándares de Base
- Limitaciones del Dictamen
  - Personas, visitas, logs, lenguajes, idioma, entorno, ...
- ANEXOS:
  - Descripción de productos / Listados de programas / Gráficos

Redacción de Dictamen (III)

1. Detalles Técnicos
   - Son "RUIDO" para el Juez
   - Si se incluyen → En ANEXOS al dictamen
   - NUNCA en Conclusiones
2. Equipo de Peritos
   - Varios Informes / Informe Único
3. BORRADOR del Dictamen
   - CONTRASTAR: Por el Colegio / Por otro Perito
     - Revisión Cruzada
     - Mantener la Confidencialidad
   - REVISAR: Por el Cliente
     - Contrastar con Abogado / Cliente
4. Notas Complementarias
   - ¿Incluirlas en Dictamen?

Redacción de Dictamen (IV)

- FIRMAR cada página
  - De las conclusiones → SIEMPRE
  - De los Anexos → ¿?
- Cabecera / Pie
  - Confidencial, nº expediente, fecha, título…
- Marcas Físicas
  - Sello → Visado del Colegio
  - ¿Muescas?
- Soporte Electrónico
  - NO obligatorio
  - Firma Digital → SIEMPRE

Entrega del Dictamen Pericial

- Se entrega a quien lo encargó
  - Al Juzgado
  - Al Cliente, no al abogado (salvo que el Cliente lo diga)

- Se entrega ORIGINAL + DOS COPIAS de:
  - DICTAMEN
  - ANEXOS
  - DOCUMENTOS
  - MATERIAL ADICIONAL

Documentación

La documentación es uno de los temas críticos en este proceso. Cualquier incorrección o incoherencia puede dar al traste con un proceso judicial abierto.

La audiencia de los entregables es variada: abogados, jueces, directivos. Esfuerzo de "adaptación de mensajes".

- Informe técnico, detallado exhaustivo y con evidencias.
- Conclusiones ejecutivas bien enfocadas legalmente.

Apoyo en proceso legal

- Preparación conjunta de preguntas y respuestas, para la vista.
- Orientación al letrado sobre aspectos técnicos.
- Declaración y aclaraciones acerca de los conceptos del peritaje.