sedian

Seguridad Digital
de Andalucía

Charla virtual

Cómo se realiza un peritaje judicial y qué funciones realiza un perito

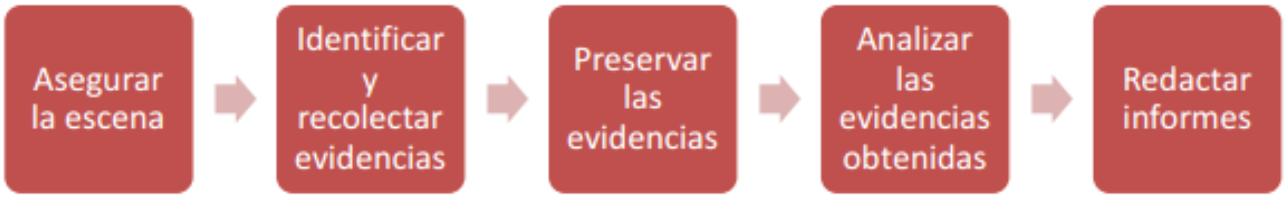
Fecha de celebración: 17 de diciembre de 2020

Junta de Andalucía

¿Qué es la informática forense?

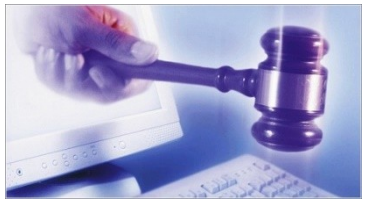
Es una ciencia de reciente aparición, que mediante procedimientos se identifican, extraen, analizan y presentan pruebas para que puedan ser aceptadas en un proceso legal.

El objetivo principal es obtener información y evidencias que se encuentran en los dispositivos físicos o virtuales.



Origen del encargo

- **Por orden judicial (designación)**:
  - Se ha de contar con:



✓Presencia de un Secretario Judicial

✓Una orden judicial

- **Por encargo privado (de parte):**
  - Se ha de contar con:

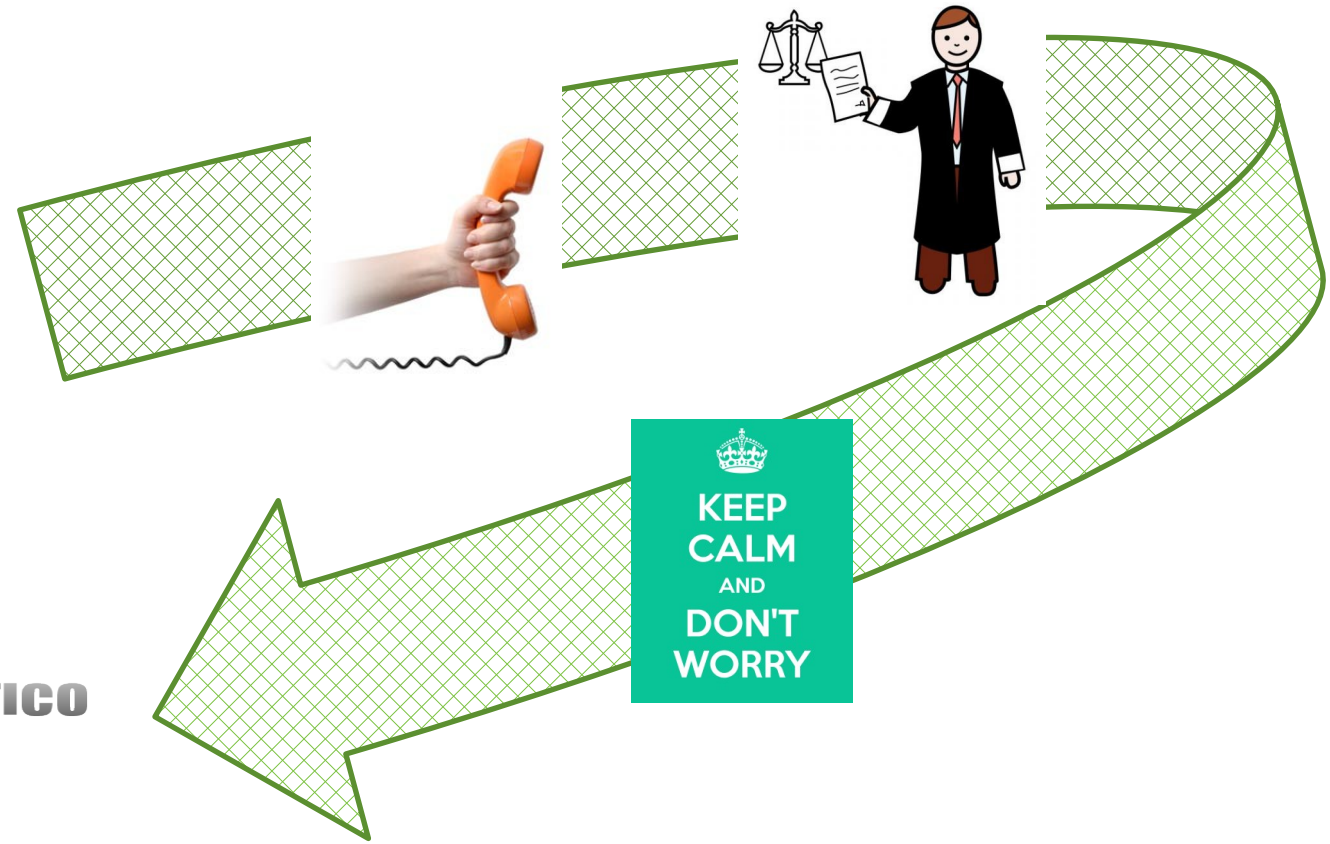
✓Presencia de un notario

✓Encargo escrito y firmado por solicitante

Origen del encargo

- Empresa DonLimpia S.L. está perdiendo ventas
- Nuevo competidor NewPro S.L. productos con mejores ofertas
- CEO de DonLimpia investiga: detrás de NewPro hay un **exempleado**
- NewPro tiene ofertas al menos 10% más baratas de DonLimpia
- Como sabe NewPro las ofertas que va a sacar DonLimpia ¿?

Caso práctico



PERITO INFORMATICO FORENSE

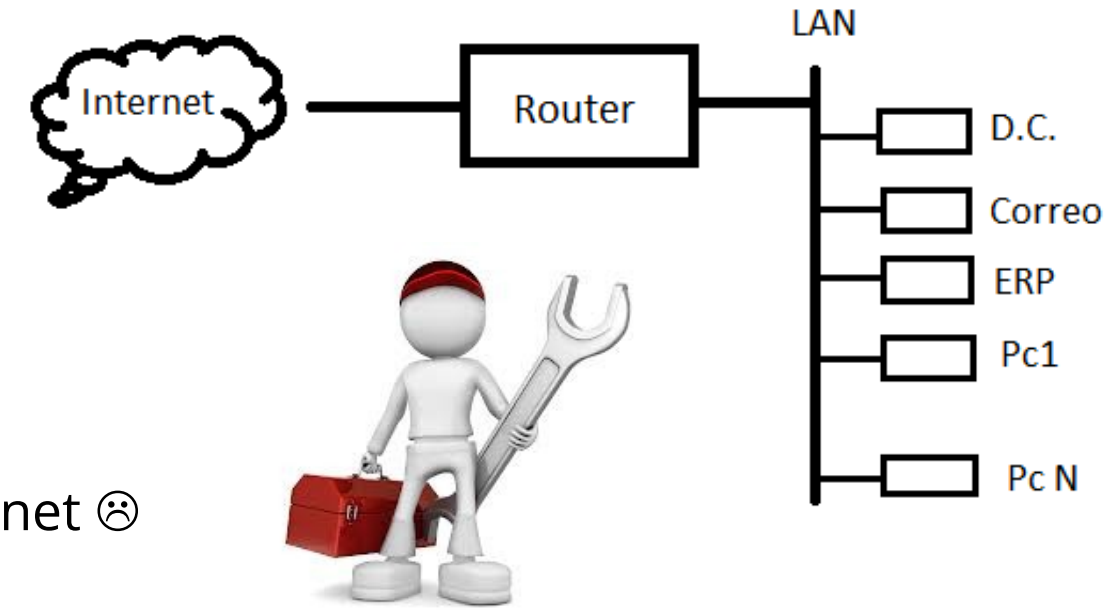
Caso práctico

- **Se convoca una reunión:**
  - Cliente (víctima)
  - Abogado
  - Perito informático
  - Técnico IT de la empresa

- **Posibles vías de fuga de información:**
  - Insiders (gente de dentro)
  - Acceso al correo electrónico
  - Trashing (indagar en basura)
  - Acceso remoto (el IT dice q es imposible...)

Caso práctico

- No hay VPN ☹
- No hay Firewall ☹
- Antivirus Caducado ☹
- Servidores expuestos a internet ☹
- …



Caso práctico

✓ **Sugerimos al IT revisar los usuarios que acceden remotamente**

- Todavía no sabemos si ha ocurrido algo en el sistema
- Llevar a cabo acciones que no supongan pérdidas o alteración de posibles evidencias
- Utilizar comandos no intrusivos

✓ **La revisión de los usuarios muestra**

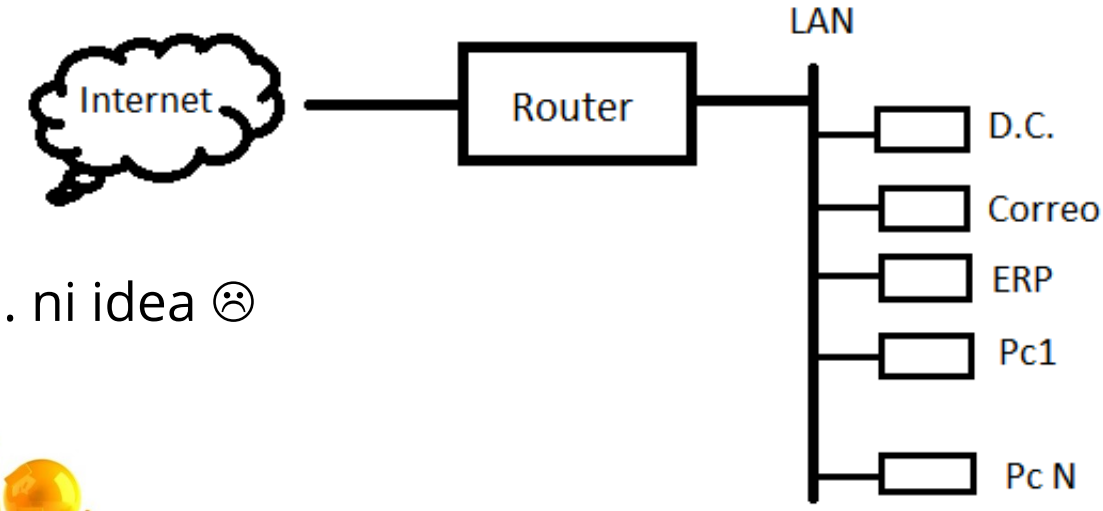
- Un usuario (*ex-trabajador*)
- **Aún está habilitado** en el grupo de administrador!!!
- Puede acceder remotamente!!. **

Caso práctico

- Ahora sabemos que estamos ante un incidente de seguridad
    - Ex-trabajador accede remotamente → Ofertas

- Como debemos proceder:
    - Identificar qué fuentes de información de las que hay en el sistema podemos analizar
    - Establecer cadena de custodia

Caso práctico



- Pedimos Pc del ex-empleado … ni idea ☹

- Optamos por analizar:
  - Server D.C.
  - Server Correo

Caso práctico: cadena de custodia

CADENA DE CUSTODIA

Procedimientos que aseguran que las evidencias no han sufrido alteración o contaminación desde su recolección, hasta el momento en el cual se presentan como prueba ante el Tribunal.

Caso práctico: cadena de custodia

- Fedatario público: Notario
- Documentar todo el proceso, fotografiando todo el entorno e Identificar unívocamente todos los dispositivos físicos y material que va a ser tomado.

Caso práctico: cadena de custodia

- Obtener una imagen del sistema bit a bit
- Notas detalladas (fechas, horas, zona horaria...)
- Minimizar cambios en la información
- Dilema: **recolección antes de análisis**
- Recolección por orden de volatilidad
- Recolección dependiendo del dispositivo

Caso práctico: cadena de custodia

- ¿Cual es la evidencia?
- ¿Cómo se consiguió?
- ¿Cuándo se adquirió?
- ¿Quién la ha gestionado?
- ¿Por qué esa persona la gestionó?
- ¿Dónde se almacenas las pruebas?

Caso práctico: problemas en la cadena de custodia

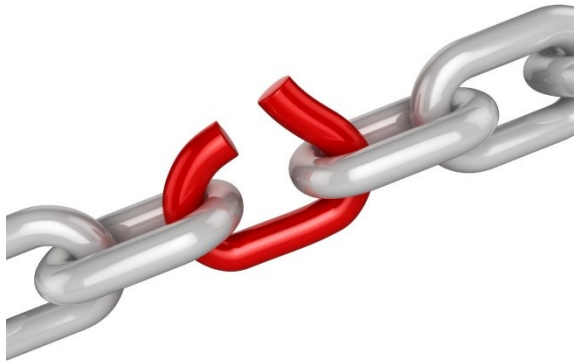
No dejar claras las personas que han intervenido

Falta de documentación

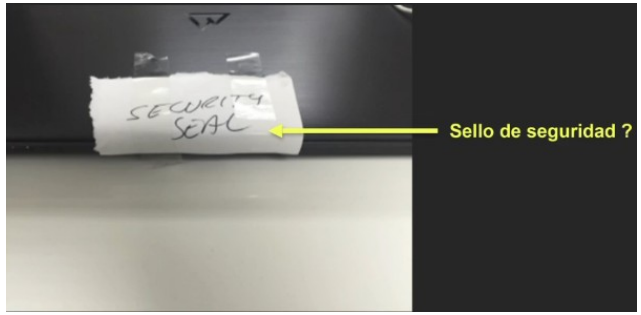
Falta de testigos

Manipular la información antes de clonarla

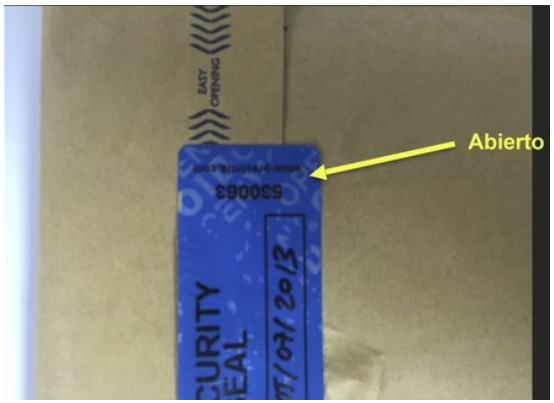
Sellado e identificación inadecuados!



Caso práctico: problemas en la cadena de custodia



Caso práctico: problemas en la cadena de custodia

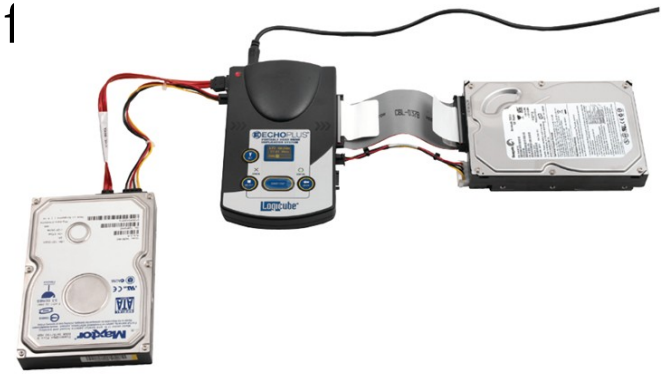


Caso práctico: adquisición de evidencias

- **Si el ordenador está encendido:**
  - **No se debe de apagar**
  - Extraer la información **volátil:**
    - Registros y contenidos de la caché
    - Conexiones de red, tablas de rutas
    - Estado de los procesos en ejecución
    - Navegadores WEB
    - Memoria RAM

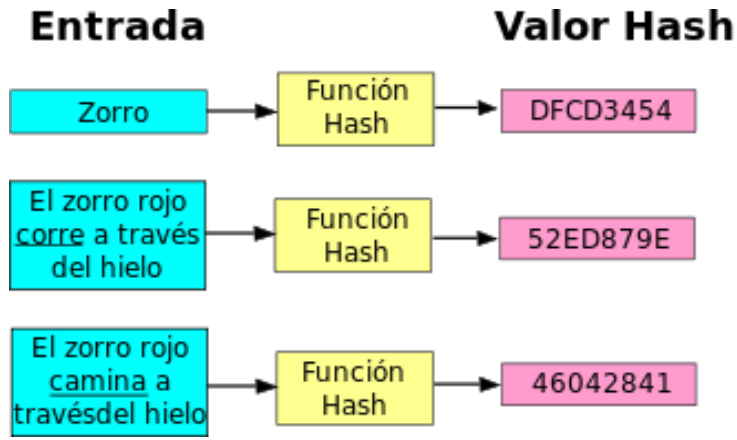
Caso práctico: adquisición de evidencias

- **Si el ordenador está apagado:**
  - No se debe encender
  - **Realizar una copia bit a bit**, (métodos f
  - Certificar mediante Hash! **
  - Nunca trabajar con los originales



Caso práctico: hash

- Algoritmo: datos entrada → salida única
- Garantiza de que las pruebas no han sido alteradas
- MD5 puede no ser admitido en un proceso judicial
- No es **reversible**



Caso práctico: fase de análisis

- Se ha de utilizar metodologías científicamente probadas.
- El análisis ha de ser sistemático, huyendo de los exámenes intuitivos.
- Los resultados deben ser reproducibles por un tercero

Caso práctico: fase de análisis

- **Intercambio de Locard →** Toda acción deja un rastro
  Es la razón de existir de la evidencia

- **Principio de Heisenberg →** Aquello que estudias lo cambias
  Es la razón de preservar la prueba original

- **Principio de la Navaja de Ockham →** La hipótesis más siempre es la más cierta
  Comenzar por lo más simple como lo más probable
  Una generalización es más probable que una especificación

sedian Seguridad Digital de Andalucía