

# Jornadas “Espacios de Ciberseguridad”

## Forense en Windows

[www.incibe.es](http://www.incibe.es)

INSTITUTO NACIONAL DE  
CIBERSEGURIDAD  
SPANISH NATIONAL  
CYBERSECURITY INSTITUTE



Esta presentación se publica bajo licencia Creative Commons del tipo:  
Reconocimiento – No comercial – Compartir Igual  
<http://creativecommons.org/licenses/by-nc-sa/4.0/>

# Índice

## 1. INCIBE - ¿Qué es?

2. Introducción a la ciberseguridad

3. Objetivos del curso

4. Contexto

5. Introducción al análisis forense

6. Tratamiento de la evidencia

7. Conceptos básicos

8. Análisis de datos volátiles en Windows

9. Análisis de datos no volátiles en Windows

10. Resumen

11. Otros datos de interés

# INCIBE - ¿Qué es?

El Instituto Nacional de Ciberseguridad de España (**INCIBE**) es una sociedad dependiente del Ministerio de Energía y Turismo y Agenda Digital (**MINETAD**) a través de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital (**SESIAD**).

INCIBE es la entidad de referencia para el desarrollo de la **ciberseguridad** y de la **confianza digital** de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos (Agenda Digital para España, aprobada en Consejo de Ministros el 15 de Febrero de 2012).

Como **centro de excelencia**, INCIBE es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia , INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.

[www.incibe.es](http://www.incibe.es)



# INCIBE - ¿Qué es?

## Pilares fundamentales sobre los que se apoya la actividad de INCIBE

- **Prestación de servicios** de protección de la privacidad, prevención y reacción a incidentes en ciberseguridad
- **Investigación** generación de inteligencia y mejora de los servicios
- **Coordinación** colaboración con entidades públicas y privadas, nacionales e internacionales

## Área de Operaciones



# Jornadas “Espacios Ciberseguridad”

## Características Jornadas

### JORNADAS PARA ALUMNOS



Alumnos de Bachiller y FP tecnológicos.  
1 temática por centro (de las 8 posibles).

Grupos de entre 20 y 30 alumnos.  
Duración 3h , en una única sesión.

<https://www.incibe.es/jornadas-incibe-espacios-ciberseguridad/estudiantes>  
**espaciosciberseguridad@incibe.es**

### JORNADAS PARA PROFESORES



Profesores de Bachiller y FP tecnológicos.  
Duración 9 horas en dos sesiones de 4,5h.

Grupos de entre 20 y 30 docentes.  
Formación para impartir las 8 temáticas de manera autónoma.

<https://www.incibe.es/jornadas-incibe-espacios-ciberseguridad/profesores>  
**espacioscs\_profesores@incibe.es**

### MATERIALES ON-LINE (YA DISPONIBLES EN LA PÁGINA WEB DE LAS JORNADAS)

PPT's de las 8 jornadas para alumnos

Videos de la impartición de las 8 jornadas íntegras

Documentación adicional para cada jornada:

Conocimientos previos de los alumnos.

Resumen de contenidos y vídeo píldoras de 5min sobre el contenido de cada jornada.

Material complementario para seguir investigando y aprendiendo sobre cada una de las materias.

Materiales para la impartición de los talleres por parte de los profesores:

PPT presentada en la jornada de **profesores**.

**Dossier completo** con la explicación detallada de todas las jornadas de alumnos así como los temas generales para la preparación de los entornos de prácticas.

#### ¿Qué temáticas se tratan en las jornadas?

Se tratará de manera monográfica una de las ocho temáticas siguientes (a decidir por parte del centro):

 <b>Mi ordenador es un zombi</b> Funcionamiento de las redes locales, así como, su proceso de creación e infección.	 <b>Programación segura de sitios web</b> Identificación de los principales requisitos a tener en cuenta para desarrollar aplicaciones web seguras.
 <b>Fundamentos del análisis de sitios Web</b> Funcionamiento de un sitio Web. Detección, identificación, análisis y forma de explotar las vulnerabilidades web.	 <b>Fundamentos del análisis de sistemas</b> Identificación, análisis y explotación de las principales vulnerabilidades de los servicios soportados por un servidor.
 <b>Análisis de malware en Android</b> Prácticas más habituales de análisis de malware en dispositivos Android.	 <b>Seguridad Wifi</b> Seguridad de los dispositivos Wifi. Funcionamiento de un punto de acceso falso.
 <b>Espionaje y cibervigilancia</b> Análisis de las diferentes técnicas y herramientas utilizadas para realizar los labores de espionaje y cibervigilancia.	 <b>Forense en Windows</b> En qué consiste y principales técnicas del análisis forense en sistemas Windows.



# Índice

1. INCIBE - ¿Qué es?
- 2. Introducción a la ciberseguridad**
3. Objetivos del curso
4. Contexto
5. Introducción al análisis forense
6. Tratamiento de la evidencia
7. Conceptos básicos
8. Análisis de datos volátiles en Windows
9. Análisis de datos no volátiles en Windows
10. Resumen
11. Otros datos de interés

# Introducción a la ciberseguridad

## Evolución de las Tecnologías de la Información

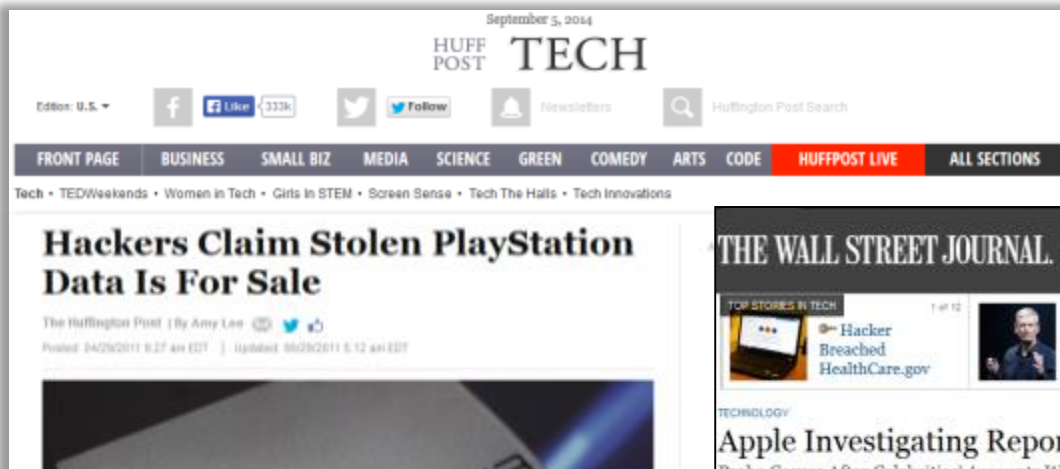
- La **información** es uno de los principales activos de una empresa.
- Las empresas almacenan y gestionan la información en los **Sistemas de Información**.
- Para una empresa resulta fundamental proteger sus Sistemas de Información para que su información esté a salvo. Dificultades:
  - El entorno donde las empresas desarrollan sus actividades es cada vez más complejo debido al desarrollo de las tecnologías de información y otros factores del entorno empresarial
  - El perfil de un ciberdelincuente de un sistema informático ha cambiado radicalmente. Si bien antes los objetivos podían ser más simples (acceder a un sitio donde nadie antes había conseguido llegar) en la actualidad los atacantes se han percatado de lo importante que es la información y sobre todo de lo valiosa que puede llegar a ser.
- Es fundamental poner los medios técnicos y organizativos necesarios para garantizar la seguridad de la información. Para lograrlo hay que garantizar la **confidencialidad**, **disponibilidad** e **integridad** de la información.





# Introducción a la ciberseguridad

## Casos notorios





# Introducción a la ciberseguridad

## Seguridad de la Información

La seguridad de la información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información:

- La **confidencialidad** es la propiedad de prevenir la divulgación de información a personas no autorizadas.
- La **integridad** es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- La **disponibilidad** es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- La **autenticidad**: la información es lo que dice ser o el transmisor de la información es quien dice ser.
- El **no repudio**: Estrechamente relacionado con la Autenticidad. Permite, en caso de ser necesario, que sea posible probar la autoría u origen de una información.



# Introducción a la ciberseguridad

## Riesgos para los Sistemas de Información

¿Qué son los riesgos en los sistemas de información?

- Las amenazas sobre la información almacenada en un sistema informático.

Ejemplos de riesgos en los sistemas de información

- **Daño físico:** fuego, agua, vandalismo, pérdida de energía y desastres naturales.
- **Acciones humanas:** acción intencional o accidental que pueda atentar contra la productividad.
- **Fallos del equipamiento:** fallos del sistema o dispositivos periféricos.
- **Ataques internos o externos:** hacking, cracking y/o cualquier tipo de ataque.
- **Pérdida de datos:** divulgación de secretos comerciales, fraude, espionaje y robo.
- **Errores en las aplicaciones:** errores de computación, errores de entrada, etc.



# Introducción a la ciberseguridad

## La figura del HACKER

¿Qué es un hacker?

Experto en seguridad informática, que se dedica a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.

¿Qué tipos de hackers existen en función de los objetivos que tienen?



**Black Hat Hackers:** Suelen quebrantar la seguridad de un sistema o una red con fines maliciosos.



**White Hat Hackers:** normalmente son los que penetran la seguridad de los sistemas bajo autorización para encontrar vulnerabilidades. Suelen ser contratados por empresas para mejorar la seguridad de sus propios sistemas.



**Gray (Grey) Hat Hackers:** Son una mezcla entre los dos anteriores puesto que tienen una ética ambigua. Normalmente su cometido es penetrar en sistemas de forma ilegal para luego informar a la empresa víctima y ofrecer sus servicios para solucionarlo.

# Introducción a la ciberseguridad

## Clases de ataques

- **Interrupción:** se produce cuando un recurso, herramienta o la propia red deja de estar disponible debido al ataque.
- **Intercepción:** se logra cuando un tercero accede a la información del ordenador o a la que se encuentra en tránsito por la red.
- **Modificación:** se trata de modificar la información sin autorización alguna.
- **Fabricación:** se crean productos, tales como páginas web o tarjetas magnéticas falsas.



# Introducción a la ciberseguridad

## Técnicas de hacking

- **Spoofing:** se suplanta la identidad de un sistema total o parcialmente.
- **Sniffing:** se produce al escuchar una red para ver toda la información transmitida por ésta.
- **Man in the middle:** siendo una mezcla de varias técnicas, consiste en interceptar la comunicación entre dos interlocutores posicionándose en medio de la comunicación y monitorizando y/o alterando la comunicación.
- **Malware:** se introducen programas dañinos en un sistema, como por ejemplo un virus, un keylogger (herramientas que permiten monitorizar las pulsaciones sobre un teclado) o rootkits (herramientas que ocultan la existencia de un intruso en un sistema).
- **Denegación de servicio:** consiste en la interrupción de un servicio sin autorización.
- **Ingeniería social:** se obtiene la información confidencial de una persona u organismo con fines perjudiciales. El Phishing es un ejemplo de la utilización de ingeniería social, que consigue información de la víctima suplantando la identidad de una empresa u organismo por internet. Se trata de una práctica muy habitual en el sector bancario.
- Adicionalmente existen multitud de ataques como **XSS**, **CSRF**, **SQL injection**, etc.

# Introducción a la ciberseguridad

## Mecanismos de defensa

Ante esta figura, ¿cómo pueden protegerse las compañías con las nuevas tecnologías?

Los principales sistemas y más conocidos son los siguientes:

- **Firewall:** sistemas de restricción de tráfico basado en reglas.
- **Sistemas IDS / IPS:** sistemas de monitorización, detección y/o prevención de accesos no permitidos en una red.
- **Honeypot:** equipos aparentemente vulnerables diseñados para atraer y detectar a los atacantes, protegiendo los sistemas realmente críticos.
- **SIEM:** sistemas de correlación de eventos y generación de alertas de seguridad.
- **Antimalware:** sistemas de detección de malware informático.





# Introducción a la ciberseguridad



**Las prácticas del taller se realizan sobre un entorno controlado.**

**Utilizar las técnicas mostradas en el presente taller sobre un entorno real como Internet, puede ocasionar problemas legales.**

# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
- 3. Objetivos del curso**
4. Contexto
5. Introducción al análisis forense
6. Tratamiento de la evidencia
7. Conceptos básicos
8. Análisis de datos volátiles en Windows
9. Análisis de datos no volátiles en Windows
10. Resumen
11. Otros datos de interés

# Objetivos del curso

## ¿Qué vamos a aprender hoy?

- En qué consiste el análisis forense de un sistema informático.
- Diferentes situaciones en las cuales se realizan este tipo de análisis.
- Conceptos básicos del análisis forense.
- Técnicas de análisis forense en sistemas Windows.
- Principales ficheros y procesos con información sensible.

## ¿Cómo lo vamos a aprender?

1. Teoría.
2. Práctica:
  - a. Ejercicios prácticos a lo largo de la presentación.
  - b. Práctica final sobre un sistema preconfigurado.



# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
- 4. Contexto**
5. Introducción al análisis forense
6. Tratamiento de la evidencia
7. Conceptos básicos
8. Análisis de datos volátiles en Windows
9. Análisis de datos no volátiles en Windows
10. Resumen
11. Otros datos de interés

# Contexto

## El papel de la tecnología en un delito

- Desde el punto de vista del uso, los dispositivos pueden:
  - ✓ Verse involucrados en un delito.
  - ✓ Ser el propio canal a través del cual se comete el delito.
- Desde el punto de vista de la persona:
  - ✓ Puede pertenecer a la víctima.
  - ✓ O al delincuente.
- Desde el punto de vista del ámbito, puede aplicar:
  - ✓ En un entorno empresarial.
  - ✓ En un entorno personal.

## La utilidad del análisis forense

- Puede ser utilizado para, gracias al análisis del dispositivo, determinar qué es lo que ha ocurrido.
- Siendo aplicable para cualquiera de las casuísticas anteriores.

# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Contexto
- 5. Introducción al análisis forense**
6. Tratamiento de la evidencia
7. Conceptos básicos
8. Análisis de datos volátiles en Windows
9. Análisis de datos no volátiles en Windows
10. Resumen
11. Otros datos de interés



# Introducción al análisis forense

## ¿Qué es el análisis forense?

- Extracción de datos de un dispositivo informático, preservando la veracidad de los datos extraídos.
- Dos enfoques de análisis forense:

### Incidentes de seguridad

- Incidentes relacionados con el hacking:
  - Robo de información
  - Intrusión en redes empresariales
  - Espionaje industrial
  - *Defacements*
  - Etc.



### Delitos

- Siempre que sirva como prueba:
  - Delitos de sangre
  - Secuestros
  - Delitos relacionados con menores
  - Etc.



# Introducción al análisis forense

## Objetivos del análisis forense

- Contestar a una serie de preguntas que aporten información relevante.
- En el caso de un forense por un incidente de seguridad:
  - ✓ ¿Quién realizó el ataque?
  - ✓ ¿Cómo y cuándo se realizó?
  - ✓ ¿Qué vulnerabilidades explotó?
  - ✓ ¿Qué hizo el intruso dentro del sistema?
- En el caso de un forense por un delito:
  - ✓ ¿Poseía algún dispositivo electrónico en el momento del delito?
  - ✓ ¿Cuáles fueron sus últimas llamadas?
  - ✓ ¿Dónde estaba en el momento del delito?
  - ✓ ¿Posee información relevante en sus dispositivos electrónicos?
  - ✓ ¿Cuáles fueron sus últimas conversaciones?



# Introducción al análisis forense

## ¿Quién realiza el análisis forense?

- Analistas forenses cualificados.
- En caso de intervenir en un proceso judicial, debe ser un perito forense certificado.

## ¿Qué valor tiene el análisis forense?

- Da respuestas ante un suceso en el que se ven involucrados dispositivos informáticos.
- Si el análisis y la preservación de las evidencias es correcta, sirve como prueba judicial.



# Introducción al análisis forense

## Tipos de análisis forense

- Análisis forense de sistemas:

- Windows
- MacOS
- Unix



- Análisis forense de redes:

- Redes Ethernet
- Redes WiFi



- Análisis forense de móviles:

- Android
- iOS



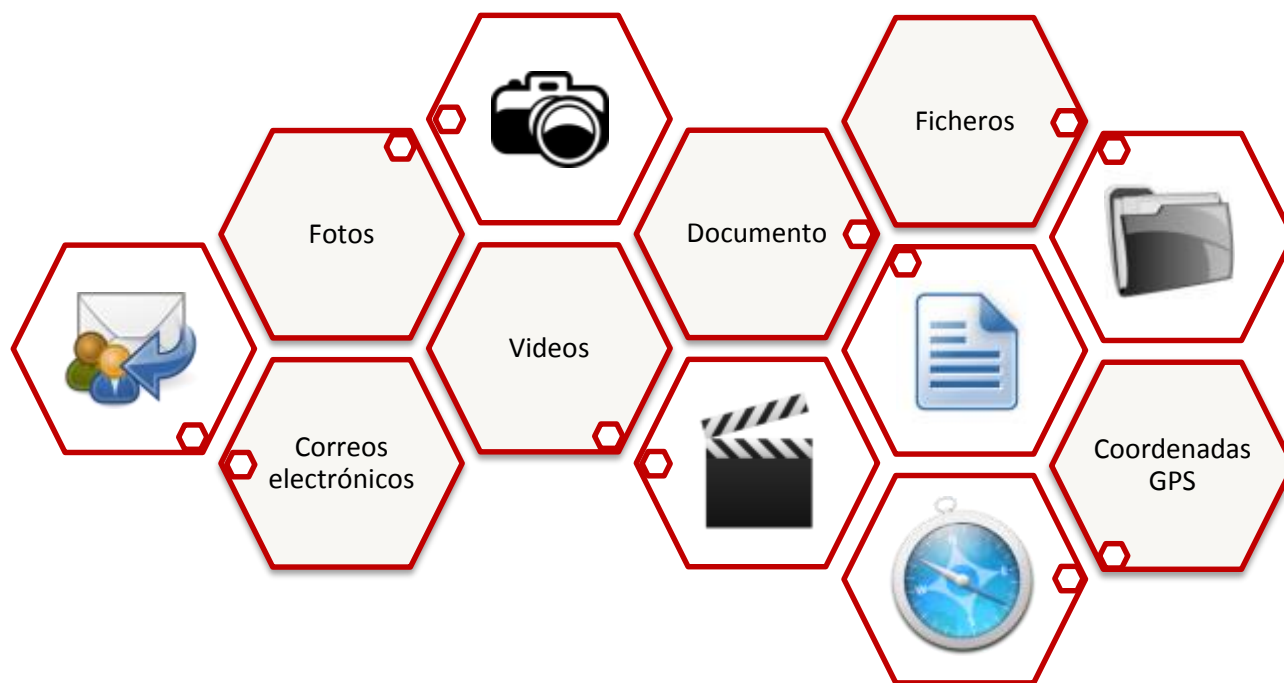
Diferentes dispositivos = diferentes técnicas

Diferentes dispositivos ≠ diferentes objetivos

# Introducción al análisis forense

## ¿Cuál es el objetivo de un análisis forense digital?

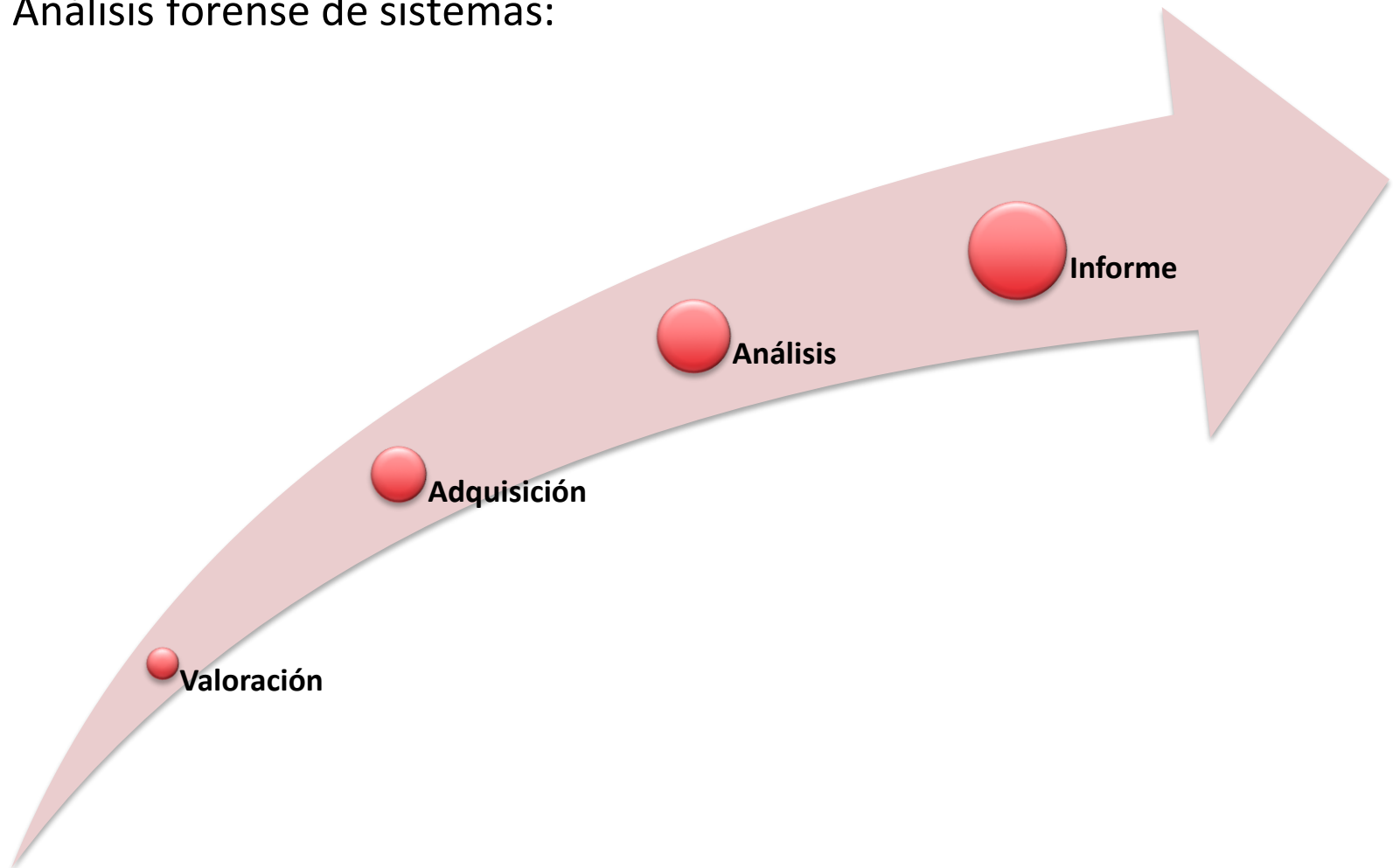
- Extraer información de un sistema de manera que sirva como evidencia digital.
- Respondiendo a las preguntas asociadas al suceso.
- Pudiendo utilizar las evidencias en un proceso judicial.
- Catalogando la información en función de su naturaleza.



# Introducción al análisis forense

## Fases del análisis forense

- Análisis forense de sistemas:





# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Contexto
5. Introducción al análisis forense
- 6. Tratamiento de la evidencia**
7. Conceptos básicos
8. Análisis de datos volátiles en Windows
9. Análisis de datos no volátiles en Windows
10. Resumen
11. Otros datos de interés

# Tratamiento de la evidencia

## ¿Qué es una evidencia digital?

- Cualquier información generada o almacenada en un sistema informático y que pueda ser utilizada en un proceso legal como prueba.
- Existen tres tipos de evidencia digital:
  - Información almacenada en el equipo informático.
  - Información generada por los equipos informáticos.
  - Información que parcialmente ha sido generada y almacenada en los equipos informáticos.
- La evidencia se debe obtener, custodiar, revisar, analizar y presentar.
- Para que tenga validez legalmente, se debe demostrar que la evidencia no ha sido alterada.

# Tratamiento de la evidencia

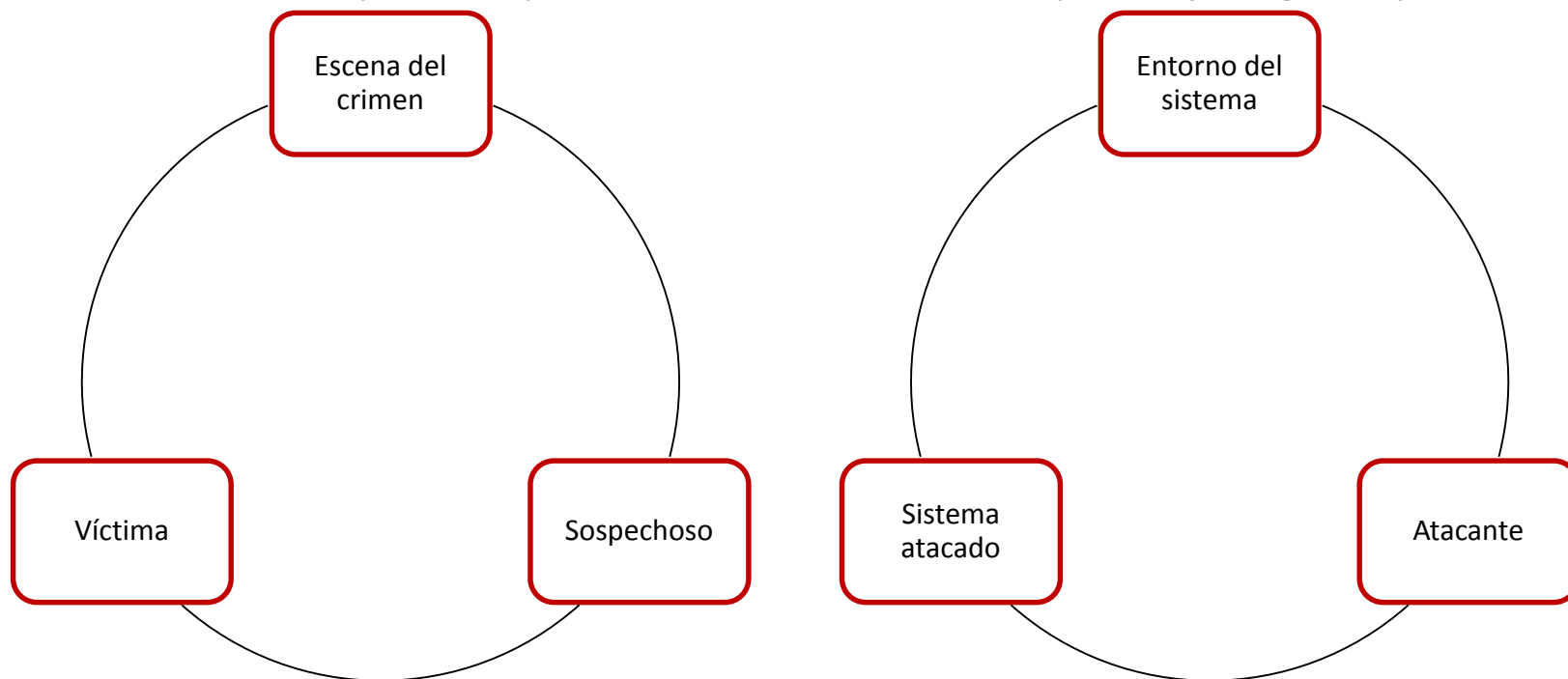
## El principio de Locard

- “Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto”



Aplicado al análisis forense...

- El uso de cualquier dispositivo informático siempre deja algún tipo de rastro.



# Tratamiento de la evidencia

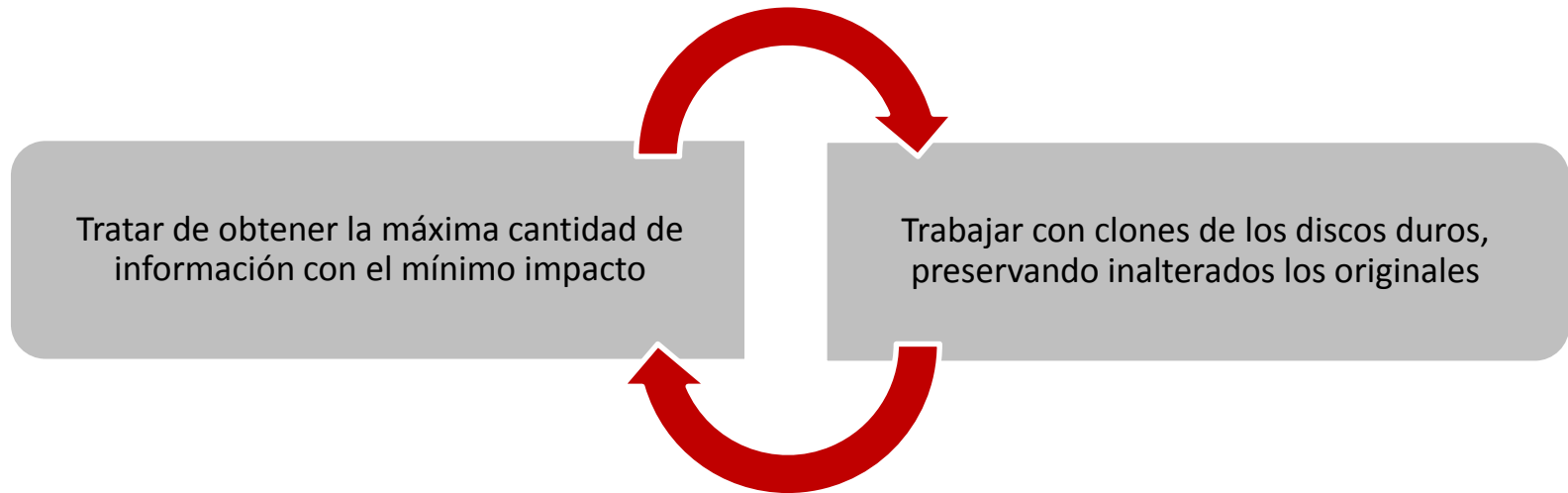
## Principio de indeterminación de Heisenberg

- “No es posible analizar algo sin que ello conlleve alguna alteración debido a la intervención del observador”



Aplicado al análisis forense...


- No es posible realizar un análisis forense de un sistema sin alterar el mismo.



# Tratamiento de la evidencia

## La cadena de custodia

- Para que las evidencias tengan validez en un proceso judicial, éstas no deben ser alteradas.
- Además, se debe demostrar la no alteración de las evidencias.
- Para ello se utiliza la cadena de custodia.
- Es un seguimiento y control de las evidencias que certifica:
  - Que la evidencia no ha sido alterada o manipulada.
  - Las personas por las que ha pasado la evidencia.
  - Detalles sobre el tratamiento de la evidencia.



**ADEPTO DIGITAL EVIDENCE  
CHAIN OF CUSTODY FORM**

Case No: 200819801 Page: of:

**ELECTRONIC MEDIA/COMPUTER DETAILS**

File No:	Description:
Media/Device:	Media No: VMware Virtual Serial No: 01000000000000000001

**IMAGE DETAILS**

Date/Time 07/16/08 11:09:02	Created By Investigator	Media Used dcfldd	Image Name hdi-1mg.dd	Segment 1
Storage Class	Total (sh1): adb6d389385c91d5c86fd2e349dc834d063c36fd			

**CHAIN OF CUSTODY**

Tracking No.	Date/Time	FROM	TO	Reason
NA	07/16/08 11:09:02	dcfldd See Hash	Investigator	Initiate Custody
		Hashing	Hashing	
		Sign	Sign	
		Hashing	Hashing	
		Sign	Sign	
		Hashing	Hashing	
		Sign	Sign	
		Hashing	Hashing	
		Sign	Sign	
		Hashing	Hashing	
		Sign	Sign	
		Hashing	Hashing	
		Sign	Sign	
		Hashing	Hashing	
		Sign	Sign	

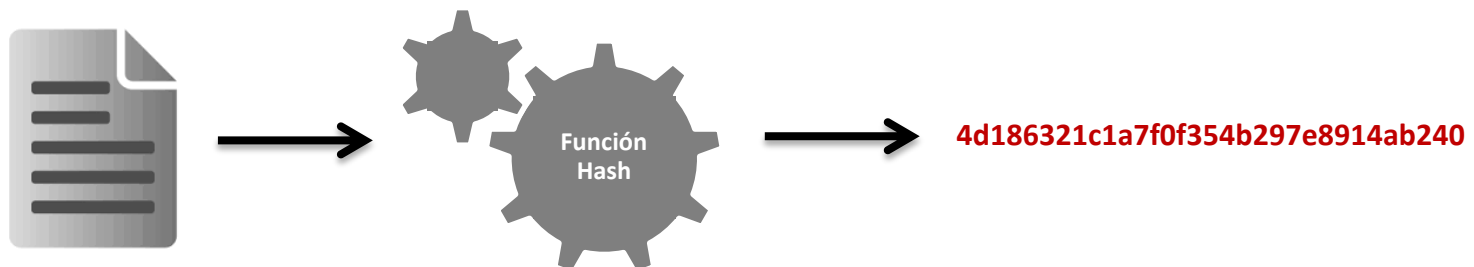
# Tratamiento de la evidencia

## ¿Cómo se justifica la no manipulación?

- Mediante la firma digital de las evidencias.
- Las evidencias deben ser copiadas y firmadas para verificar que se mantienen inalterables durante el proceso de análisis forense.

## ¿Qué es una firma digital?

- Una cadena alfanumérica que se obtiene tras aplicar un algoritmo, llamada función hash o función resumen, a un fichero origen y que identifica inequívocamente al mismo.



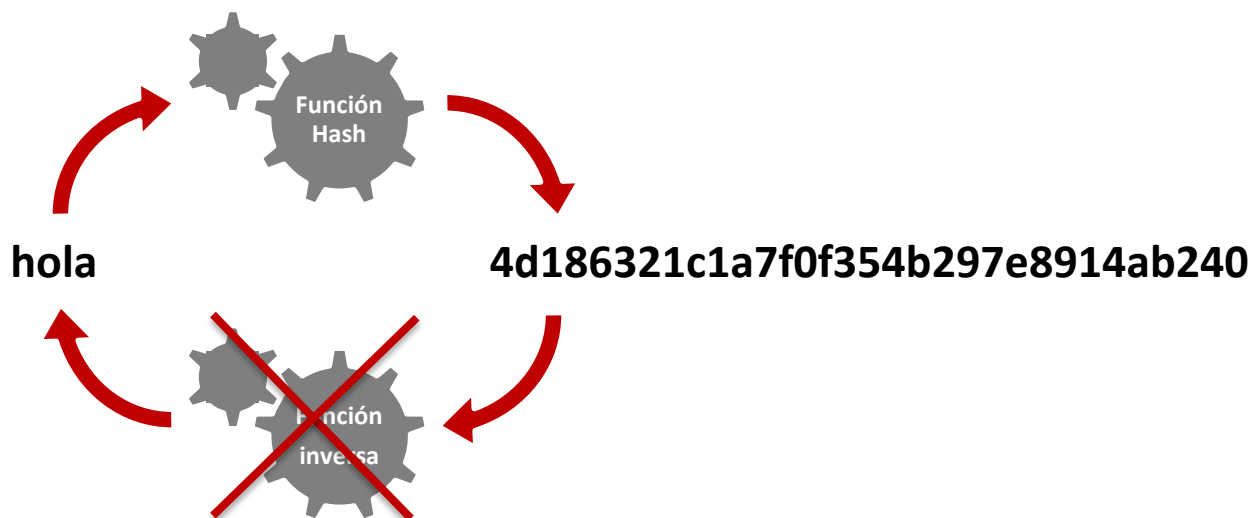
- Existen varios algoritmos de hashing: MD5, SHA1, SHA2, etc.



# Tratamiento de la evidencia

## ¿Cómo se realiza la firma digital?

- Existen gran cantidad de herramientas para firmar ficheros:
  - HashMyFiles
  - HashCalc
- Gran parte de los softwares de clonación permiten calcular el hash de los elementos clonados:
  - FTK Imager
  - DD
- Las funciones hash no son reversibles:



# Tratamiento de la evidencia

## Práctica: Firmando digitalmente un fichero

- Crear un fichero de texto con cualquier contenido:  
*echo "contenido" > nombre\_del\_fichero.txt*
- Calcular el hash MD5 de dicho fichero con la herramienta md5sum:  
*md5sum nombre\_del\_fichero.txt*
- Anotar el hash MD5 devuelto.
- Modificar el fichero original.
- Calcular de nuevo el hash del fichero modificado.
- Comparar el hash MD5 del fichero original y del fichero modificado.

```
root@eylab:~# echo "Hola, esto es una prueba" > documento.txt
root@eylab:~# md5sum documento.txt
4f31d2b2910d865484a1a4d85e0e3304 documento.txt
root@eylab:~# echo "Hola, esto es una pruebaa" > documento.txt
root@eylab:~# md5sum documento.txt
7b87fdc fb5860d9382eec3c6c9able25 documento.txt
root@eylab:~#
```

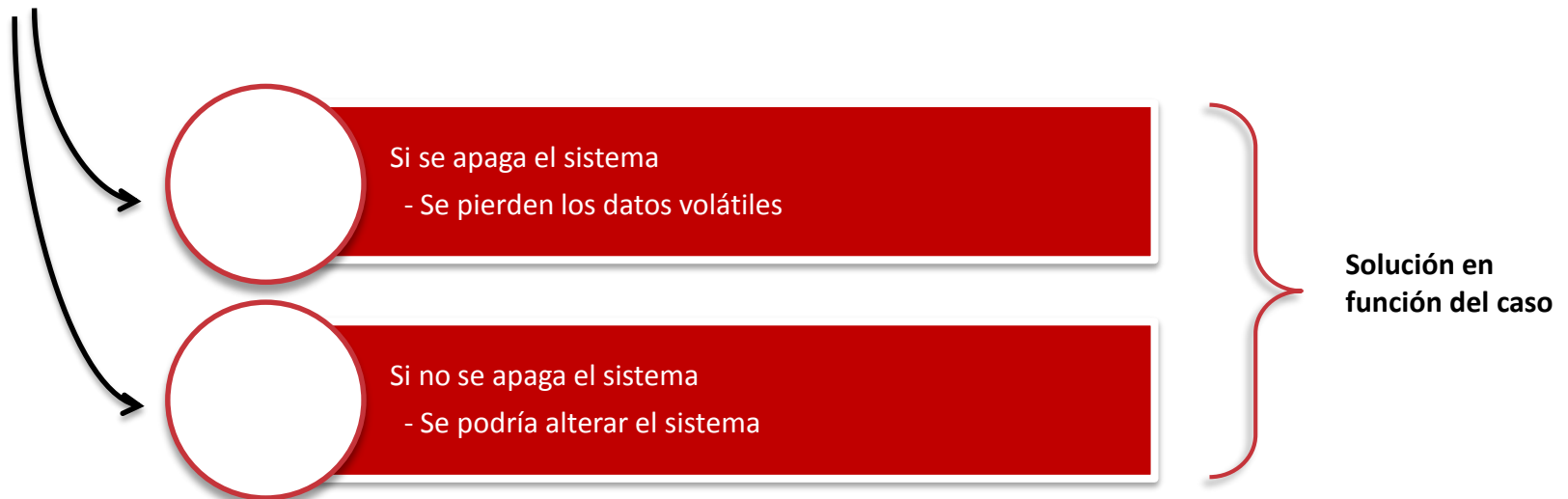
# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Contexto
5. Introducción al análisis forense
6. Tratamiento de la evidencia
- 7. Conceptos básicos**
8. Análisis de datos volátiles en Windows
9. Análisis de datos no volátiles en Windows
10. Resumen
11. Otros datos de interés

# Conceptos básicos

## Tipos de entorno de análisis

- Si nos encontramos el dispositivo encendido: Análisis en caliente
  - Podemos recoger información de la memoria volátil.
  - Es sencillo contaminar el sistema de manera involuntaria.
- Si nos encontramos el sistema apagado: Análisis post mortem
  - Evitamos una alteración de las evidencias del sistema.
  - Sólo seremos capaces de recopilar información persistente.
- Entonces, si la máquina está encendida... ¿es recomendable apagar?



# Conceptos básicos

## Tipos de datos

- Volátiles:
  - Servicios en ejecución.
  - Usuarios autenticados.
  - Ficheros en uso.
  - Procesos de memoria.
- No volátiles:
  - Ficheros.
  - Documentos.
  - Logs.
- Transitorios:
  - Memoria.
  - Caché.
- Frágiles:
  - Archivos temporales.

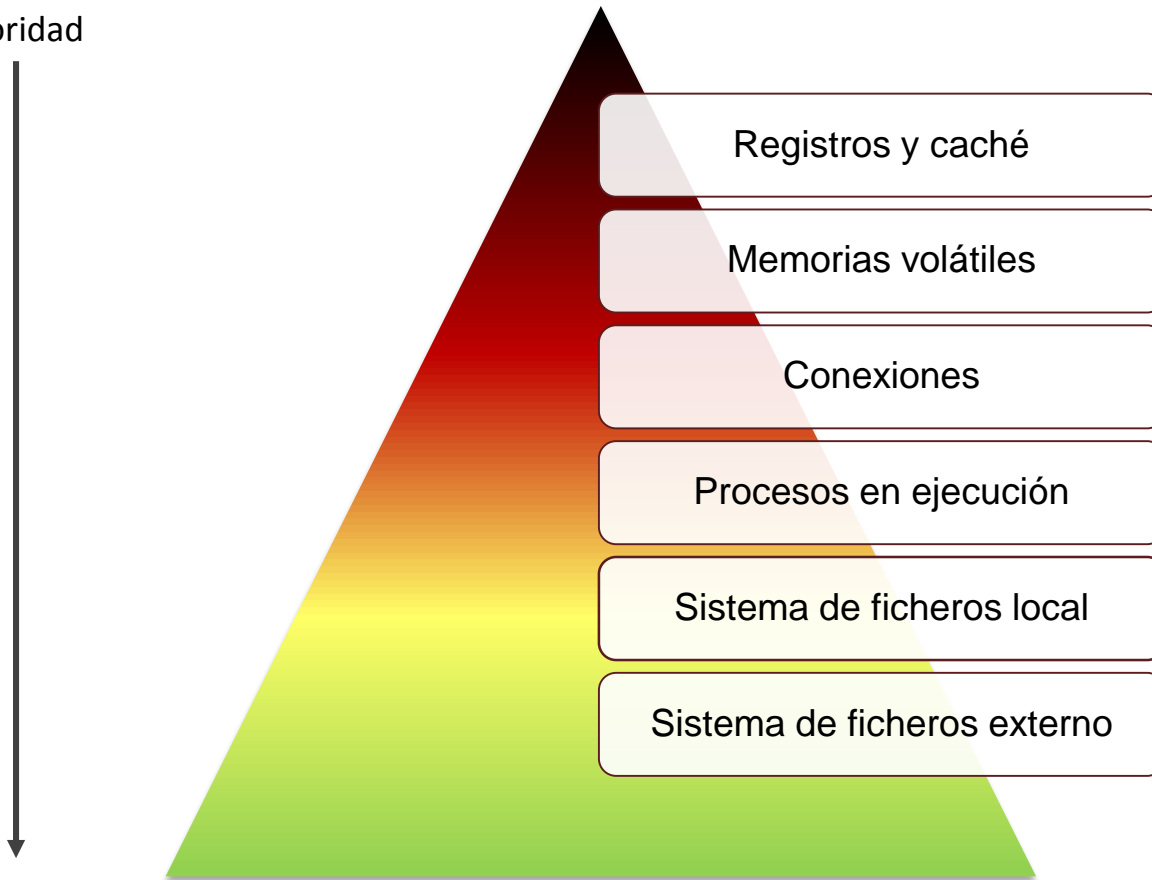


# Conceptos básicos

## Volatilidad

- ¿Qué es?
  - La capacidad de persistencia en el tiempo de los datos.

Prioridad



# Conceptos básicos

## Clonado del disco

- ¿Por qué se realiza?
  - Para evitar alterar la muestra original.
- ¿Qué es el clonado?
  - Copia idéntica del disco duro original.
- ¿Es lo mismo que realizar una imagen de un disco duro?
  - La imagen sólo almacena ficheros.
  - No almacena otro tipo de sectores o información del disco duro.



# Conceptos básicos

## Práctica: Clonando un pendrive

- Conectar el pendrive a clonar.
- Ver los dispositivos conectados con el comando:

```
sudo -fdisk -l
```

- Anotar la referencia del dispositivo del tipo:

```
/dev/sdb1
```

- Ejecutar el clonado del dispositivo a una imagen:

```
dd if=/dev/sdb1 of=/root/backup.dd
```

```
Disk /dev/sdb: 4057 MB, 4057989120 bytes
236 heads, 63 sectors/track, 533 cylinders, total 7925760 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

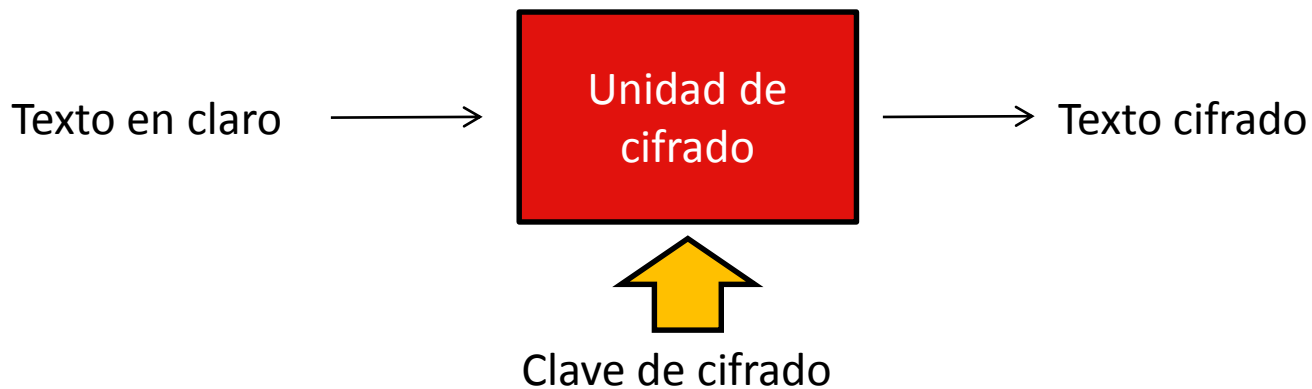
   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1   *          32       7925759      3962864    b   W95 FAT32
root@eylab:~# dd if=/dev/sdb1 of=/root/Desktop/back.dd
7925728+0 registros leídos
7925728+0 registros escritos
4057972736 bytes (4,1 GB) copiados, 222,104 s, 18,3 MB/s
root@eylab:~#
```



# Conceptos básicos

## ¿Y si el disco está cifrado?

- Es común utilizar herramientas de cifrado para proteger los datos:
  - Bitlocker
  - TrueCrypt
- ¿Cómo nos afecta a la hora de analizar un disco cifrado?
  - La clonación es posible.
  - Sin embargo, no veremos información legible.
- ¿Cómo actuamos entonces?
  - Es necesario obtener la clave de cifrado para poder analizarlo.
  - Obtención mediante fuerza bruta.



# Conceptos básicos

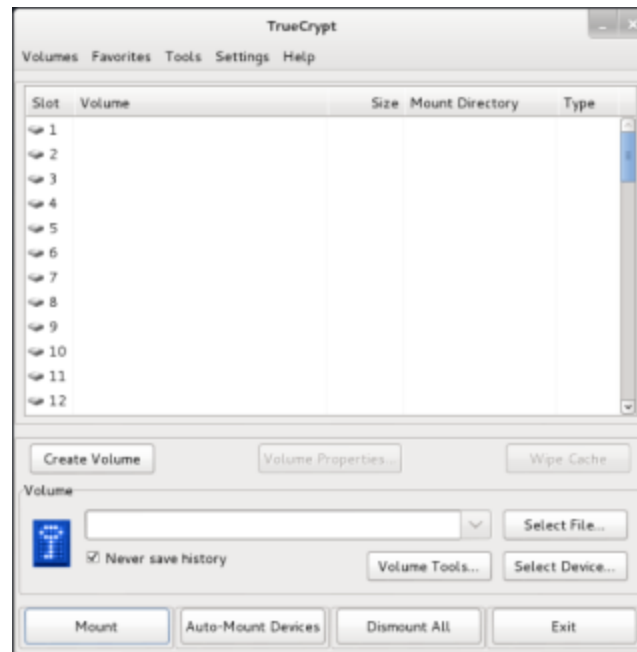
## Práctica: Fuerza bruta en ficheros cifrados (I)

- Creamos un fichero de texto:

*echo "texto" > nombre\_fichero.txt*

- Ciframos el fichero con TrueCrypt, arrancando la herramienta con el siguiente comando y siguiendo las indicaciones:

*truecrypt*



# Conceptos básicos

## Práctica: Fuerza bruta en ficheros cifrados (II)

- Realizamos fuerza bruta contra el fichero mediante TrueCrack y un diccionario en el cual estará la contraseña elegida:

*truecrack -t nombre\_fichero -c alfabeto -m longitud\_máxima -v*

```
root@eylab:~# truecrack -t /root/prueba -c abc -m 3 -v
TrueCrack v3.0
Website: http://code.google.com/p/truecrack
Contact us: infotruecrack@gmail.com

Memory initialization...

COUNT    PASSWORD    RESULT
0          a           NO
1          b           NO
2          c           NO
3          aa          NO
4          ba          NO
5          ca          NO
6          ab          NO
7          bb          NO
8          cb          NO
9          ac          NO
10         bc          NO
11         cc          NO
12         aaa         YES
No found password
Total computations:    "13"
root@eylab:~#
```

# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Contexto
5. Introducción al análisis forense
6. Tratamiento de la evidencia
7. Conceptos básicos
- 8. Análisis de datos volátiles en Windows**
9. Análisis de datos no volátiles en Windows
10. Resumen
11. Otros datos de interés

# Análisis de datos volátiles en Windows

## ¿Qué información nos aportan los datos volátiles?

- Los datos volátiles de Windows nos darán información acerca de:
  - Usuarios.
  - Conexiones.
  - Memoria.
  - Servicios.

## Herramientas

- Para realizar el análisis de datos volátiles, es necesario utilizar herramientas especiales.
- Podemos utilizar herramientas nativas o no nativas del sistema operativo.
- Nativas: herramientas y comandos de Windows que nos darán información importante sobre la configuración y el estado del sistema:
  - Ipconfig.
  - Route.
- No nativas: herramientas especializadas para el diagnóstico de sistemas Windows:
  - Suite Sysinternals.

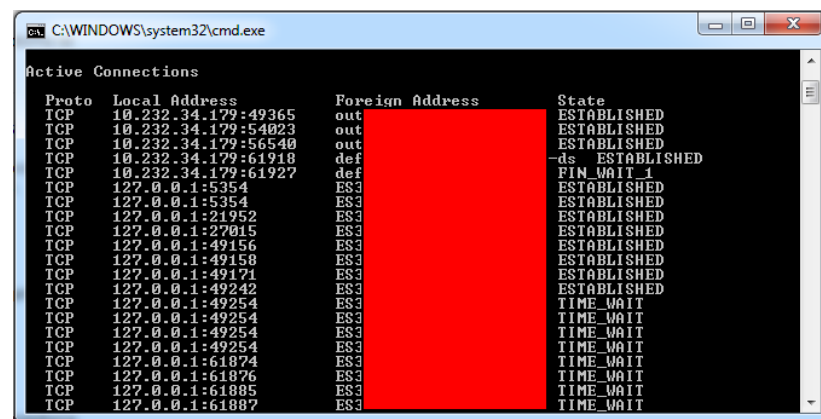
# Análisis de datos volátiles en Windows

## Conexiones

- Uno de los elementos volátiles más importantes son las conexiones abiertas del sistema.
- Estas conexiones se pierden al apagar el equipo.
- Existen herramientas nativas de Windows para visualizar las conexiones abiertas.

## Herramientas y comandos nativos

- Netstat → Puertos y conexiones abiertas.
- Nbtstat → Conexiones de NetBIOS.
- Net → Recursos compartidos.
- Route → Configuración de la red.
- Ipconfig → Interfaces de red.



Proto	Local Address	Foreign Address	State
TCP	10.232.34.179:49365	out	ESTABLISHED
TCP	10.232.34.179:54023	out	ESTABLISHED
TCP	10.232.34.179:56540	out	ESTABLISHED
TCP	10.232.34.179:61910	def	ESTABLISHED
TCP	10.232.34.179:61927	def	FIN_WAIT_1
TCP	127.0.0.1:5354	ES3	ESTABLISHED
TCP	127.0.0.1:5354	ES3	ESTABLISHED
TCP	127.0.0.1:21952	ES3	ESTABLISHED
TCP	127.0.0.1:27015	ES3	ESTABLISHED
TCP	127.0.0.1:49156	ES3	ESTABLISHED
TCP	127.0.0.1:49158	ES3	ESTABLISHED
TCP	127.0.0.1:49171	ES3	ESTABLISHED
TCP	127.0.0.1:49242	ES3	ESTABLISHED
TCP	127.0.0.1:49254	ES3	TIME_WAIT
TCP	127.0.0.1:49254	ES3	TIME_WAIT
TCP	127.0.0.1:49254	ES3	TIME_WAIT
TCP	127.0.0.1:49254	ES3	TIME_WAIT
TCP	127.0.0.1:61874	ES3	TIME_WAIT
TCP	127.0.0.1:61876	ES3	TIME_WAIT
TCP	127.0.0.1:61885	ES3	TIME_WAIT
TCP	127.0.0.1:61887	ES3	TIME_WAIT

# Análisis de datos volátiles en Windows

## Práctica: Análisis de conexiones (I)

- Abrimos una consola de Windows:

*C:\Windows\System32\cmd.exe*

- Puertos y conexiones abiertos:

*netstat -a*

- Tráfico por proceso:

*netstat -b*

- Estadísticas de conexiones:

*netstat -es*

- Conexiones de NetBIOS:

*nbtstat -r*

# Análisis de datos volátiles en Windows

## Práctica: Análisis de conexiones (II)

- Caché de NetBIOS:

*nbtstat -c*

- Configuración de la red:

*route PRINT*

- Interfaces de red:

*ipconfig /all*

- Recursos compartidos:

*net SHARE*



# Análisis de datos volátiles en Windows

## Usuarios

- Los usuarios activos también se consideran un elemento volátil.
- Existen herramientas nativas de Windows para visualizar los usuarios.
- También existen otras herramientas que extraen el hash de la contraseña e incluso en texto plano.

## Herramientas y comandos nativos

- Nbtstat → Usuarios de NetBIOS.
- Net → Usuarios de recursos compartidos.

## Herramientas externas

- Suite Sysinternals → Usuarios externos conectados.

# Análisis de datos volátiles en Windows

## Práctica: Análisis de usuarios

- Abrimos una consola de Windows:

`C:\Windows\System32\cmd.exe`

- Usuarios de NetBIOS:

`nbtstat -n`

- Usuarios de recursos compartidos:

`net USERS`

- Usuarios locales y remotos:

`[ruta]/sysinternals/PsLoggedon.exe`

- SID de usuarios:

`[ruta]/sysinternals/PsGetsid.exe`

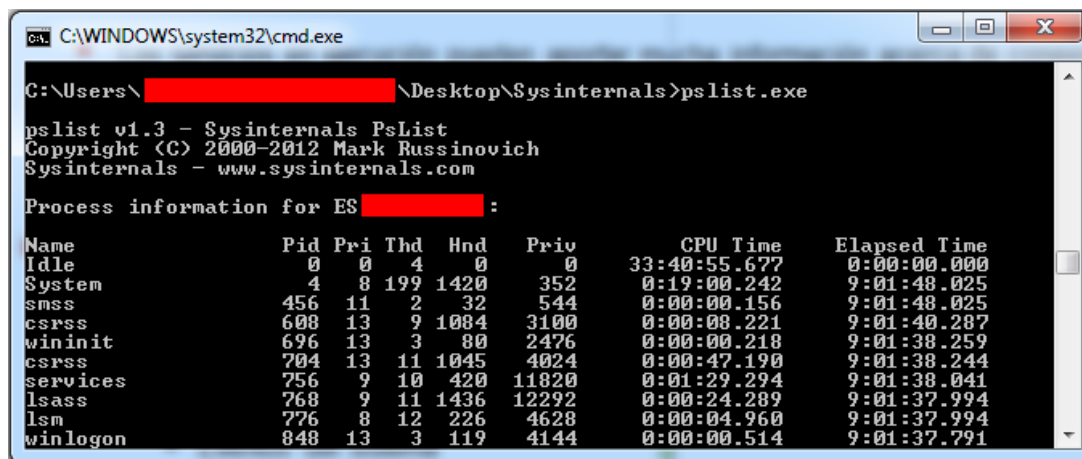
# Análisis de datos volátiles en Windows

## Servicios

- Los servicios en ejecución pueden aportar mucha información acerca de conexiones maliciosas.
- Es imprescindible analizarlos antes de apagar el equipo.

## Herramientas externas

- Suite Sysinternals:
  - Servicios en ejecución y procesos activos.
  - Eventos del sistema.



```
C:\WINDOWS\system32\cmd.exe

C:\Users\[redacted]\Desktop\Sysinternals>pslist.exe

pslist v1.3 - Sysinternals PsList
Copyright (C) 2000-2012 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for ES [redacted]:

Name                Pid Pri Thd  Hnd   Priv    CPU Time    Elapsed Time
-----
Idle                 0   0   4    0     0    33:40:55.677  0:00:00.000
System               4   8  199  1420   352    0:19:00.242  9:01:48.025
smss                 456  11   2    32    544    0:00:00.156  9:01:48.025
csrss                608  13   9  1084   3100    0:00:08.221  9:01:40.287
wininit              696  13   3    80    2476    0:00:00.218  9:01:38.259
csrss                704  13  11  1045   4024    0:00:47.190  9:01:38.244
services             756   9  10   420  11820    0:01:29.294  9:01:38.041
lsass                768   9  11  1436  12292    0:00:24.289  9:01:37.994
lsn                  776   8  12   226   4628    0:00:04.960  9:01:37.994
winlogon             848  13   3   119   4144    0:00:00.514  9:01:37.791
```

# Análisis de datos volátiles en Windows

## Práctica: Análisis de servicios

- Abrimos una consola de Windows:

*C:\Windows\System32\cmd.exe*

- Servicios en ejecución:

*[ruta]/sysinternals/PsService.exe*

- Procesos activos:

*[ruta]/sysinternals/PsList.exe*

- Eventos del sistema:

*[ruta]/sysinternals/PsLoglist.exe*

# Análisis de datos volátiles en Windows

## Memoria RAM

- La memoria RAM es una fuente muy importante de información en un proceso forense.
- La información, además de volátil, es frágil, pues se libera y se reasigna de forma dinámica.

## Herramientas externas

- MDD → Volcado de la memoria RAM
- Volatility → Framework para el análisis de un volcado RAM



# Análisis de datos volátiles en Windows

## Práctica: Análisis de memoria RAM (I)

- Abrimos una consola de Windows:  
*C:\Windows\System32\cmd.exe*
- Realizamos un volcado de la memoria sobre un fichero:  
*[ruta]/mdd\_1.3.exe -o fichero\_de\_volcado.img*
- Analizamos el volcado con Volatility.

```
Process: lsass.exe Pid: 1928 Address: 0x80000
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x00080000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ.....
0x00080010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  .....@.....
0x00080020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0x00080030  00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00  .....

0x80000 4d          DEC EBP
0x80001 5a          POP EDX
0x80002 90          NOP
0x80003 0003        ADD [EBX], AL
0x80005 0000        ADD [EAX], AL
0x80007 000400      ADD [EAX+EAX], AL
0x8000a 0000        ADD [EAX], AL
0x8000c ff       DB 0xff
0x8000d ff00     INC DWORD [EAX]
0x8000f 00b800000000  ADD [EAX+0x0], BH
0x80015 0000        ADD [EAX], AL
0x80017 004000      ADD [EAX+0x0], AL
```

# Análisis de datos volátiles en Windows

## Práctica: Análisis de memoria RAM (II)

- Información del volcado:

*volatility -f [ruta]/ fichero\_de\_volcado.img imageinfo*

- Procesos ocultos:

*volatility -f [ruta]/ fichero\_de\_volcado.img psxview*

- Árbol de procesos:

*volatility -f [ruta]/ fichero\_de\_volcado.img pstree*

- Procesos huérfanos

*volatility -f [ruta]/ fichero\_de\_volcado.img psscan*

- Conexiones

*volatility -f [ruta]/ fichero\_de\_volcado.img connscan*

# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Contexto
5. Introducción al análisis forense
6. Tratamiento de la evidencia
7. Conceptos básicos
8. Análisis de datos volátiles en Windows
- 9. Análisis de datos no volátiles en Windows**
10. Resumen
11. Otros datos de interés



# Análisis de datos no volátiles en Windows

## ¿Qué información nos aportan los datos no volátiles?

- Los datos no volátiles de Windows nos darán información acerca de:
  - Logs.
  - Ficheros.
  - Emails.
  - Información relevante.
  - Etc.

## Herramientas

- Para realizar el análisis de datos no volátiles, en muchas ocasiones no es necesario utilizar herramientas específicas.
- Existen herramientas para recuperar ficheros borrados.
- Algunas herramientas: Hfind, Recuva Free, Exiftool, Foca Free...

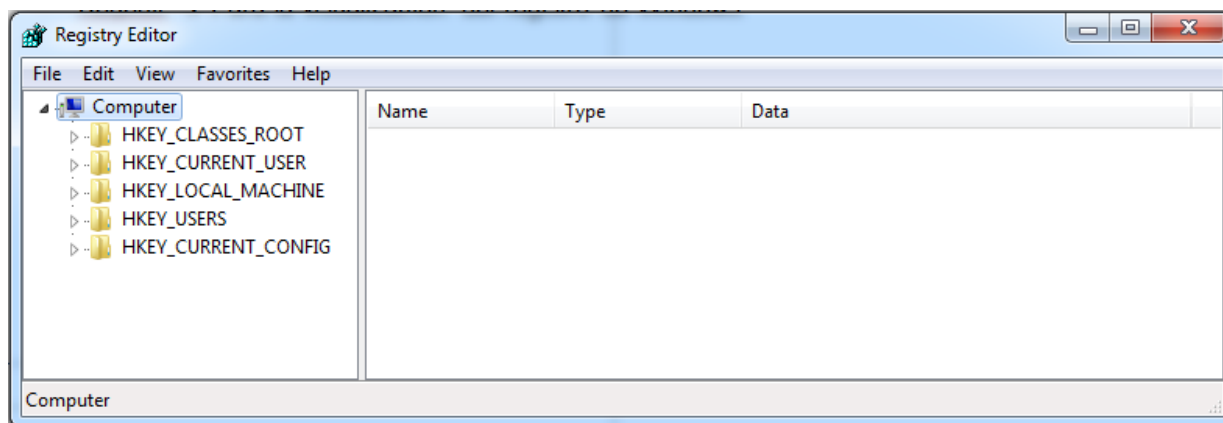
# Análisis de datos no volátiles en Windows

## Registros

- El registro de Windows almacena información sobre:
  - Configuraciones.
  - Programas ejecutados en el arranque.
  - Propiedades de usuarios.
  - Etc.

## Herramientas nativas

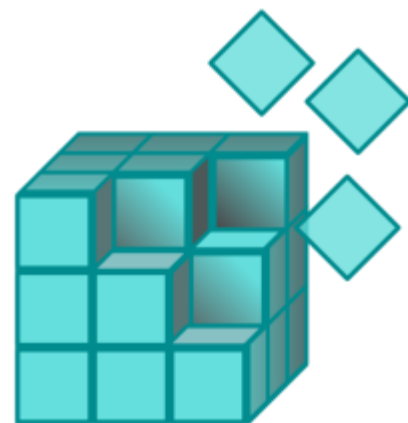
- Regedit → Para la visualización del registro de Windows.



# Análisis de datos no volátiles en Windows

## Práctica: Análisis del Registro

- Abrimos el editor del registro:  
*C:\Windows\regedit.exe*
- Análisis de los registros de configuración del usuario actual:  
*HKEY\_CURRENT\_USER*
- Análisis de los registros de configuración de otros usuarios:  
*HKEY\_USERS*
- Análisis de los registros de configuración del sistema:  
*HKEY\_LOCAL\_MACHINE*



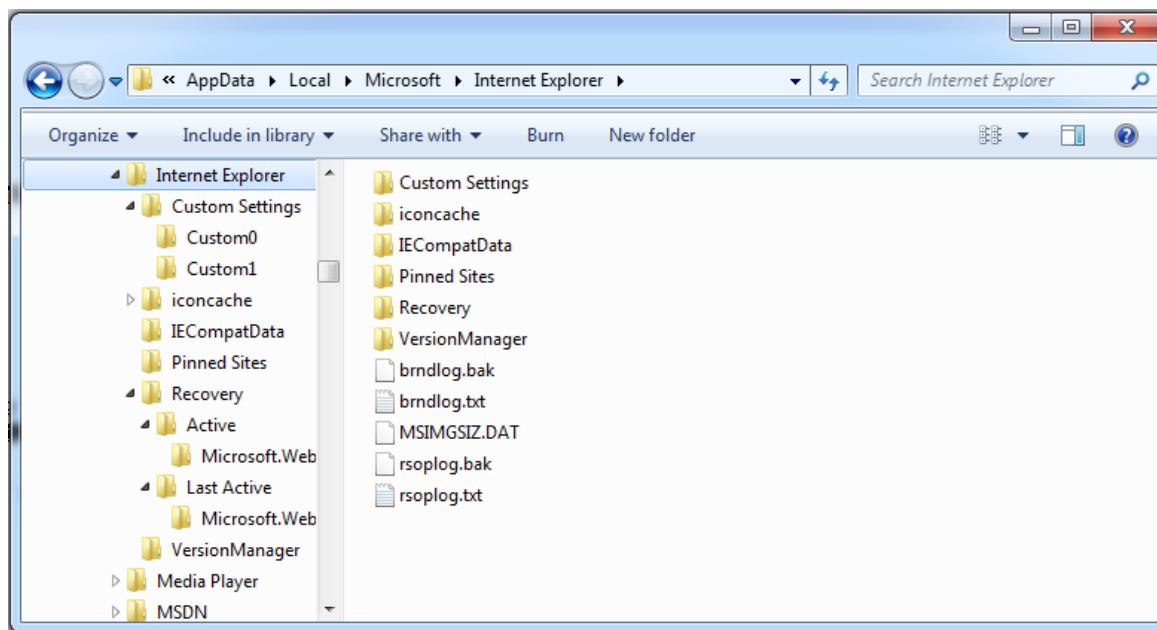
# Análisis de datos no volátiles en Windows

## Historial de navegación

- El historial de navegación aporta datos acerca de las páginas web visitadas.
- Cada navegador almacena el historial en rutas diferentes.

## Herramientas nativas

- Notepad → Visualización de ficheros en texto plano



# Análisis de datos no volátiles en Windows

## Práctica: Análisis del historial de navegación

- Abrir el explorador de Windows.
- Navegar hasta las rutas de los diferentes navegadores.  
*C:\Users\<usuario>\AppData\Local\<navegador>*
- Analizar con Notepad los ficheros caché.
- Analizar con Notepad cualquier fichero susceptible de contener información relevante.

## Práctica: Forense del navegador Firefox

- Localizar la ruta de Firefox con los perfiles de usuario.
- Ejecutar el comando:  
*python dumpzilla.py [ruta]\directorio\_del\_perfil --All*

# Análisis de datos no volátiles en Windows

## Ficheros temporales

- Los ficheros temporales pueden almacenar información relevante acerca de ficheros recientes y software del sistema.
- Se consideran ficheros frágiles debido a su capacidad de eliminación.

## Herramientas nativas

- Debido a la naturaleza de este tipo de ficheros, normalmente se utilizan programas comunes para su visualización.
  - Imágenes.
  - Videos.
  - Ficheros de texto.
  - Documentos PDF.
  - Ejecutables.
  - Logs.
  - Etc.

# Análisis de datos no volátiles en Windows

## Práctica: Análisis de ficheros temporales

- Abrir el explorador de Windows.
- Navegar hasta la ruta de ficheros temporales:  
*C:\Users\<usuario>\AppData\Local\Temp*
- Explorar la carpeta en busca de archivos con información relevante:
  - Imágenes.
  - Videos.
  - Ficheros de texto.
  - Documentos PDF.



# Análisis de datos no volátiles en Windows

## Backup de emails

- Algunas aplicaciones de correo electrónico almacenan un backup de emails.
- Los correos electrónicos suelen ser una de las fuentes con más información relevante.

## Herramientas

- Para abrir este tipo de ficheros, normalmente es necesaria la aplicación nativa.
- En el caso de Outlook, sería necesario disponer de la herramienta o de una herramienta que analice los archivos PST/OST y muestre su información en texto plano.
- Ejemplo:
  - Outlook almacena un backup de emails en la ruta:  
*C:\Users\<usuario>\AppData\Local\Microsoft\Outlook*





# Análisis de datos no volátiles en Windows

## Metadatos

- Los documentos almacenan información adicional en el propio fichero.
- Esta información puede contener:
  - Usuario creador.
  - Fecha de creación.
  - Fecha de modificación.
  - Software utilizado.

## Herramientas

- Exiftool → Para sistemas Linux o Windows.
- Foca Free → Para sistemas Windows.
- Propiedades del fichero.



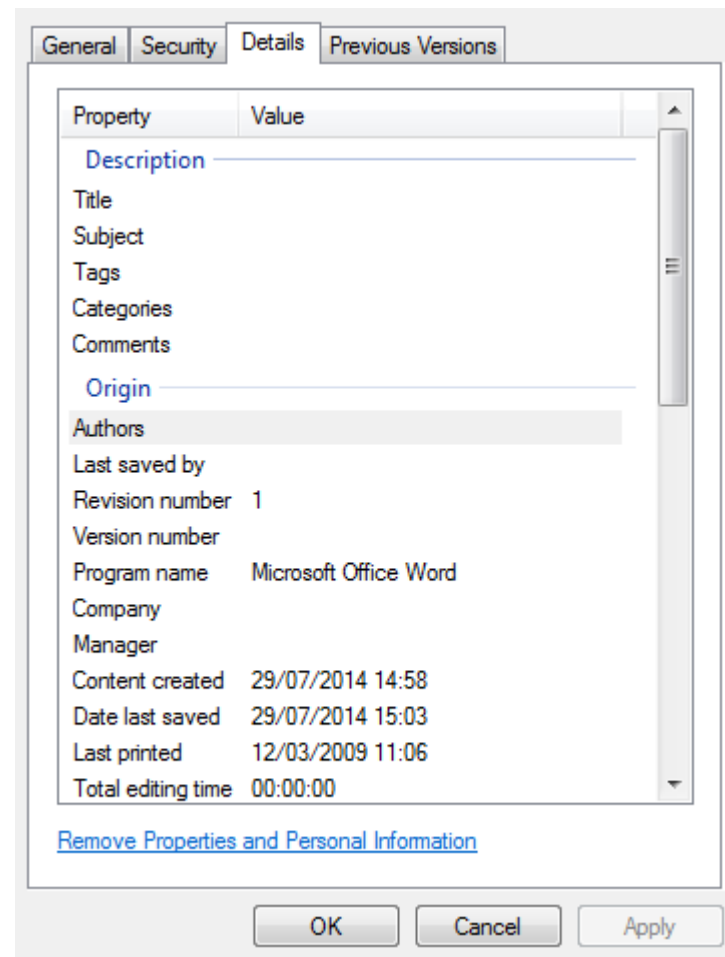
# Análisis de datos no volátiles en Windows

## Práctica: Análisis de metadatos

- Crear un documento con una herramienta ofimática.
- Seleccionar el fichero y visualizar sus propiedades.
- En la pestaña “detalles”, analizar los metadatos del fichero.

## Práctica: Eliminar metadatos

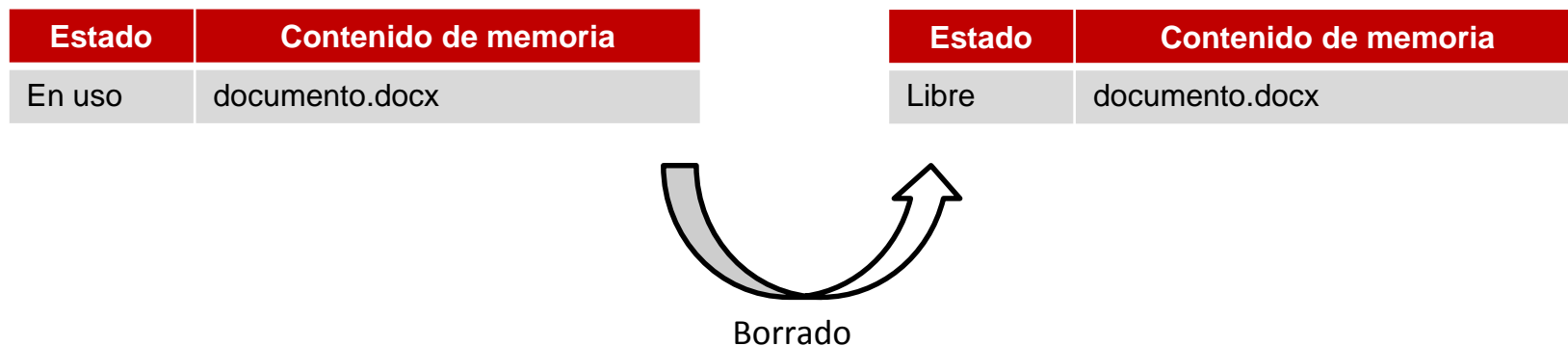
- En la pestaña “detalles” seleccionar la eliminación de propiedades e información personal.
- Verificar la correcta eliminación de los metadatos.



# Análisis de datos no volátiles en Windows

## Recuperar ficheros eliminados

- Cuando se elimina un fichero, éste no es eliminado de la memoria.
- El espacio que ocupa se marca como libre, pero la información sigue existiendo.
- Hasta que el espacio de memoria no se sobrescribe, es posible recuperar el fichero original.



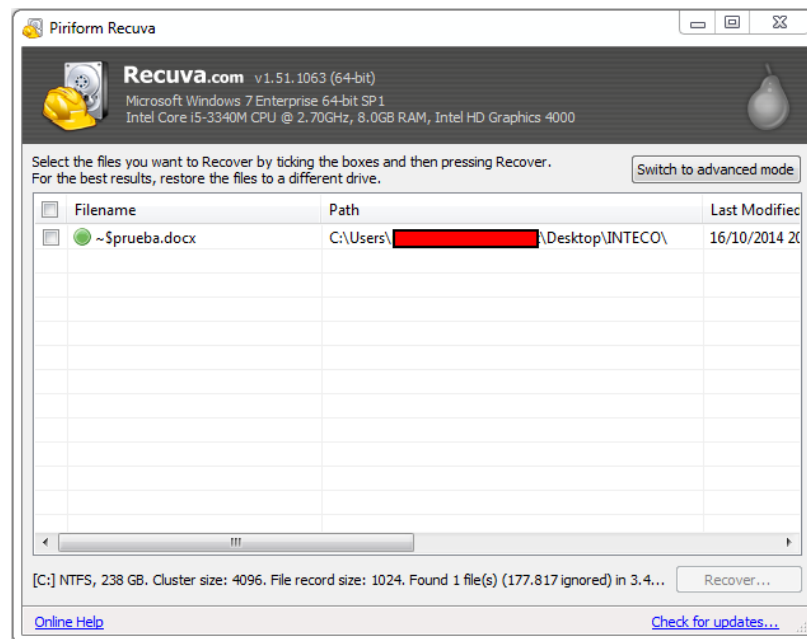
## Herramientas

- Recuva Free → Recuperación de ficheros eliminados.

# Análisis de datos no volátiles en Windows

## Práctica: Recuperar ficheros

- Crear un documento con una herramienta ofimática.
  - Eliminar el fichero.
  - Abrir la herramienta Recuva Free.
  - Seleccionar la ruta a analizar.
  - Seleccionar todos los tipos de archivo.
  - Verificar los resultados y recuperar el fichero.
- 
- A tener en cuenta:
    - Para eliminar completamente los ficheros, se pueden utilizar herramientas como Eraser.
    - Estos programas sobrescriben la memoria con datos aleatorios.



# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Contexto
5. Introducción al análisis forense
6. Tratamiento de la evidencia
7. Conceptos básicos
8. Análisis de datos volátiles en Windows
9. Análisis de datos no volátiles en Windows

## 10. Resumen

11. Otros datos de interés

# Resumen

## Resumen de conceptos

- El análisis forense de sistemas informáticos pretende responder a varias preguntas acerca de un suceso.
- Con el tratamiento adecuado, las evidencias extraídas pueden ser utilizadas en un proceso judicial.
- Hay que poner los medios necesarios para no alterar el sistema analizado.
- Es importante planificar el proceso de análisis:
  - Primero datos volátiles.
  - Posteriormente datos no volátiles.
- Los procedimientos de análisis de sistemas que no sean Windows son conceptualmente similares.
- Únicamente varían las herramientas y los procesos de obtención.

# Resumen

## Cuestiones

1. ¿Qué es la cadena de custodia de una evidencia digital? ¿Por qué es útil?
2. ¿Por qué se recomienda clonar el disco antes de analizarlo?
3. ¿Qué se recomienda extraer primero, los datos volátiles o no volátiles?
4. ¿La memoria RAM es información volátil o no volátil?
5. ¿Qué son los metadatos? ¿Qué información pueden almacenar?

# Resumen

## Respuestas


1. Es un seguimiento y control de las evidencias ante la validación de un proceso judicial que certifica: que la evidencia no ha sido alterada o manipulada, las personas por las que ha pasado la evidencia, y los detalles sobre el tratamiento de la evidencia.
2. Para evitar alterar la muestra original.
3. Se recomienda extraer primero los datos volátiles, que son aquellos que estarán disponibles durante un menor periodo de tiempo y que son más susceptibles de ser modificados o desaparecer.
4. La memoria RAM es información volátil.
5. Los documentos almacenan información adicional en el propio fichero, estos son los metadatos, pueden contener la siguiente información: usuario creador, fecha de creación, fecha de modificación y software empleado.



# Índice

1. INCIBE - ¿Qué es?
2. Introducción a la ciberseguridad
3. Objetivos del curso
4. Contexto
5. Introducción al análisis forense
6. Tratamiento de la evidencia
7. Conceptos básicos
8. Análisis de datos volátiles en Windows
9. Análisis de datos no volátiles en Windows
10. Resumen
- 11. Otros datos de interés**

# Encuesta de satisfacción



INSTITUTO NACIONAL DE CIBERSEGURIDAD

**Jornadas Ciberseguridad - alumnos**  
Encuesta de satisfacción que rellenarán los alumnos que asistan a las Jornadas de Ciberseguridad de Alumnos

0%   
100%

**Datos generales**  
Datos de información general sobre las personas encuestadas , centro de estudios donde se realizan las jornadas, etc

**\* Jornada:**  
Seleccione una de las siguientes opciones

Por favor escoja... ▼

**Fecha de la jornada:**

**Hora de inicio de la jornada**  
Seleccione una de las siguientes opciones

Por favor escoja... ▼

**\* Nombre de tu centro de estudios**

**\* Provincia**


**Estudios en curso**  
Seleccione una de las siguientes opciones

Por favor escoja... ▼

**\* Edad**  
Sólo se pueden introducir números en este campo.

**\* Sexo**

☐ Femenino ☐ Masculino



# Otras Actuaciones de interés

Si te gusta la ciberseguridad y quieres profundizar en este tema en INCIBE se están desarrollando las siguientes actividades y eventos de ciberseguridad:



**Formación especializada en ciberseguridad:** MOOC que se desarrollan a través de la plataforma de formación de INCIBE (<https://www.incibe.es/formacion>) sobre conceptos avanzados en ciberseguridad tales como ciberseguridad industrial, seguridad en dispositivos móviles, programación segura, malware y sistemas TI.



**Programa de becas:** Programa de becas anual en el que se establecerán diferentes tipologías de becas: formación de cursos especializados y másteres en ciberseguridad, y becas de investigación. Todas las publicaciones de este tipo se realizará a través de la siguiente página: <https://www.incibe.es/ayudas>



**Evento de ciberseguridad – CyberCamp** (<http://cybercamp.es>).

CyberCamp es el evento internacional de INCIBE para **identificar**, **atraer** y **promocionar el talento** en ciberseguridad.

Identificar trayectorias profesionales de los jóvenes talento.

Detectar y promocionar el talento mediante talleres y retos técnicos.

Atraer el talento ofreciendo conferencias y charlas de ciberseguridad por profesionales y expertos de primer nivel.

Y muchas cosas más....

Evento para **familias**, contando con actividades de concienciación y difusión de la ciberseguridad para padres, educadores e hijos.

Promoción de la **industria** e **investigación** en ciberseguridad.

Gracias  
por tu atención

Contáctanos

**Contacto (más información y dudas sobre las jornadas):**



**[espaciosciberseguridad@incibe.es](mailto:espaciosciberseguridad@incibe.es)**

**En las redes sociales:**



@Incibe  
@Certs\_  
@Osiseguridad  
@CyberCampES  
@CyberEmprende\_



Oficina de Seguridad del internauta  
CyberCamp



INCIBE  
OSIseguridad



Pág. INCIBE  
Grupo INCIBE

**En la sede:**

Avenida José Aguado, 41 - Edificio INCIBE  
24005 León  
Tlf. 987 877 189

**En los sitios web:**

[www.incibe.es](http://www.incibe.es)  
[www.osi.es](http://www.osi.es)  
[www.cybercamp.es](http://www.cybercamp.es)  
[www.certs.es](http://www.certs.es)

[www.incibe.es](http://www.incibe.es)

INSTITUTO NACIONAL DE  
CIBERSEGURIDAD  
SPANISH NATIONAL  
CYBERSECURITY INSTITUTE



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE ENERGÍA, TURISMO  
Y AGENDA DIGITAL