La prueba informática: instrumentos y metodología relativos al análisis forense de discos duros y de redes

Michele Ferrazzano
michele@informaticaforense.it

SEGUNDA SESIÓN
Seminario de Informática Forense
16 de mayo de 2012
Sala de Juntas (Facultad de Derecho)

La prueba científica digital: la computer forensics

- La prueba es cualquier instrumento, método, persona, cosa o circunstancia que pueda proporcionar información útil para resolver la falta de certeza en torno a la verdad o falsedad de los hechos (Taruffo)
- Cuando la prueba se refiere a un hecho regido por leyes científicas y/o técnicas especializadas para las que es necesario recurrir a un experto, nos encontramos en el ámbito de la prueba científica
- La computer forensics tiene su origen en ámbientes ligados al common law y con un alto grado de evolución tecnológica, como los EEUU
- Existen agencias especializadas que certifican
  - software
  - hardware

  empleado para la investigación

La prueba científica digital: la computer forensics

- Pero, ¿qué se entiende por prueba científica en el caso de la informática?

- Partimos de la siguiente base

dato informático

y

bit

El dato informático

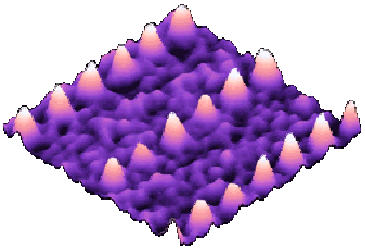
- Se trata de una secuencia de bits, contenidos en un dispositivo capaz de memorizarlos

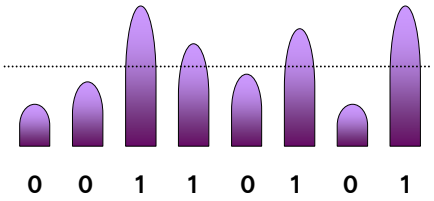
- El bit es la unidad de medida de la información
  - Es una cifra binaria, vale cero (0) o uno (1)

- Estamos acostumbrados a trabajar con archivos
  - Un archivo es una suma lógica de bits

El dato informático

- El bit es intangibile
- El bit es un estado de la materia
  - Por ejemplo, en el caso de soportes magnéticos (discos duros)
  - El bit necesita un soporte sobre el que ser memorizado

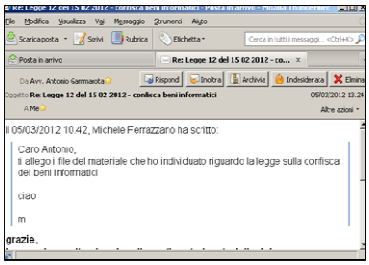




El dato informático

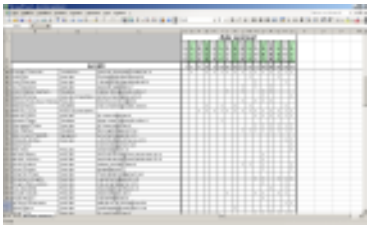
- Ejemplo
  - HOLA → 01001000010011110100110001000001
- Ha existido al menos un momento en el que tales bits estaban grabados en un dispositivo, cuyo estado podía ser modificado por un operador, impertiendo las órdenes oportunas
- Es imposible constatar eventuales modificaciones realizadas en cada bit
  - Entonces, ¿debe entenderse que el dato no es fiable
    - No. Por ejemplo: firma digital

El dato informático (algunos ejemplos)



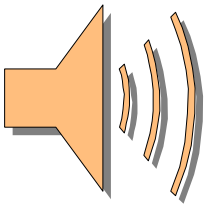
Email

Video



Folio electrónico

Sonido



El dato informático

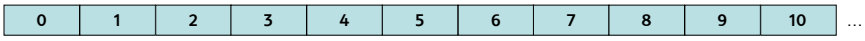
- ¿Puede considerarse dato informático un archivo contenido en un disco duro?
  - Sí, pero es reductivo
- En un disco duro es posible descubrir numerosos elementos útiles para reconstruir la escena del crimen (o para verificar las coartadas de algunos sujetos)
  - Datos eliminados
    - Archivos cancelados, espacio no utilizado, slack space
  - Metadatos
  - Fecha de último acceso, última modificación, creación de archivos
  - …

El dato informático
Gestión de los archivos en un disco duro

- Un disco duro está organizado de forma lógica mediante el uso de un sistema de archivos
  - El sistema de archivos divide el espacio disponible en el disco duro en sectores de iguales dimensiones
  - Cuando se graba un archivo, se usa el menor número posible de sectores, pero siempre en número suficiente para guardar el archivo

El dato informático
Gestión de los archivos en un disco duro

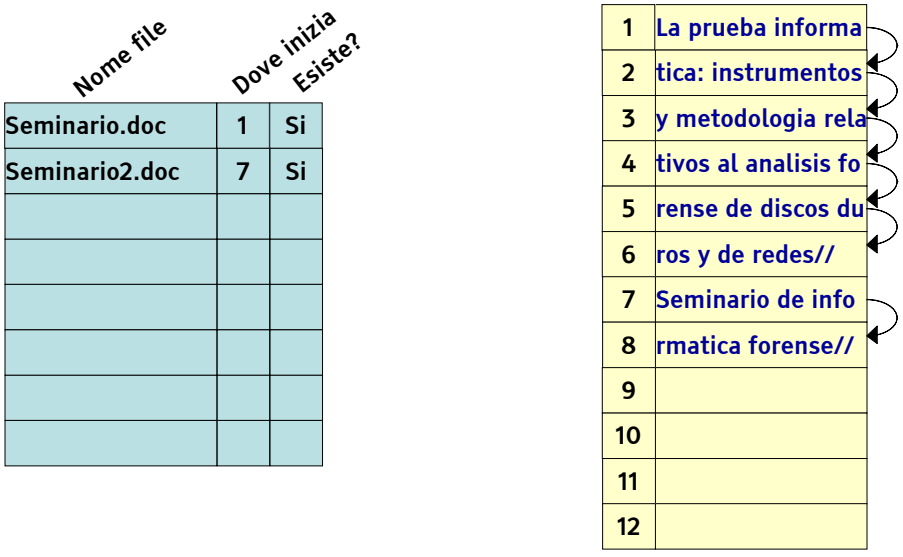
- Ejemplo (el disco duro está dividido en secciones de 2048 byte)



- Un archivo de 1 bytes ocupa 1 sector
- Un archivo de 2047 bytes ocupa 1 sectores
- Un archivo de 2049 bytes ocupa 2 sectores
- Un archivo de 10000 bytes ocupa 5 sectores

El dato informático
Gestión de los archivos en un disco duro

El dato informático
Gestión de los archivos en un disco duro



El dato informático
Gestión de los archivos en un disco duro

Nome file	Dove inizia	Esiste?
Seminario.doc	1	No
Seminario2.doc	7	Si

Ejemplo de cancelación de un archivo

En realidad, el archivo permanece en el discoduro

1	La prueba informa
2	tica: instrumentos
3	y metodologia rela
4	tivos al analisis fo
5	rense de discos du
6	ros y de redes//
7	Seminario de info
8	rmatica forense//
9	
10	
11	
12	

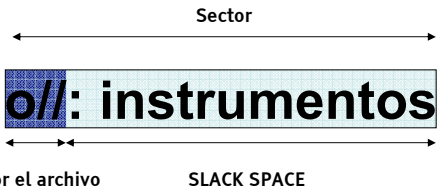
El dato informático
Gestión de los archivos en un disco duro

Nome file	Dove inizia	Esiste?
Nome.doc	1	Si
Seminario2.doc	7	Si

1	Michele Ferrazzan
2	o//: instrumentos
3	y metodologia rela
4	tivos al analisis fo
5	rense de discos du
6	ros y de redes//
7	Seminario de info
8	rmatica forense//
9	
10	
11	
12	

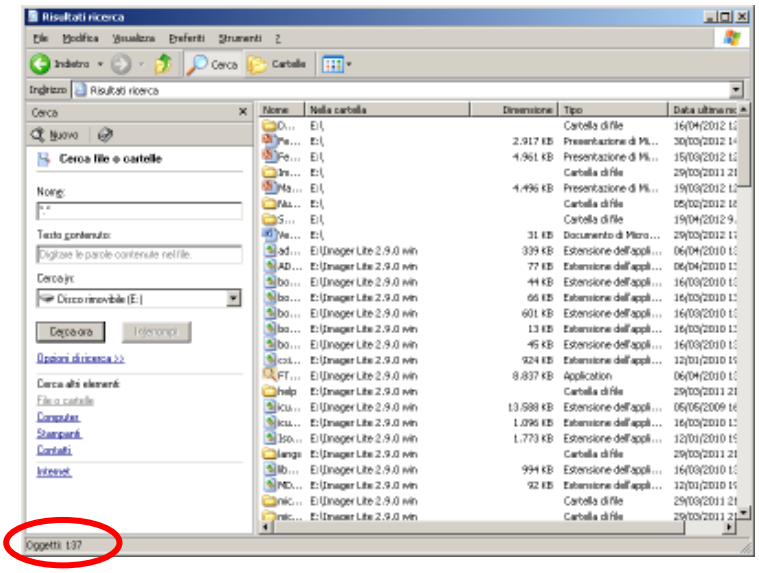
El dato informático
Gestión de los archivos en un disco duro

- Algunos datos pueden sobrevivir durante años en el slack space



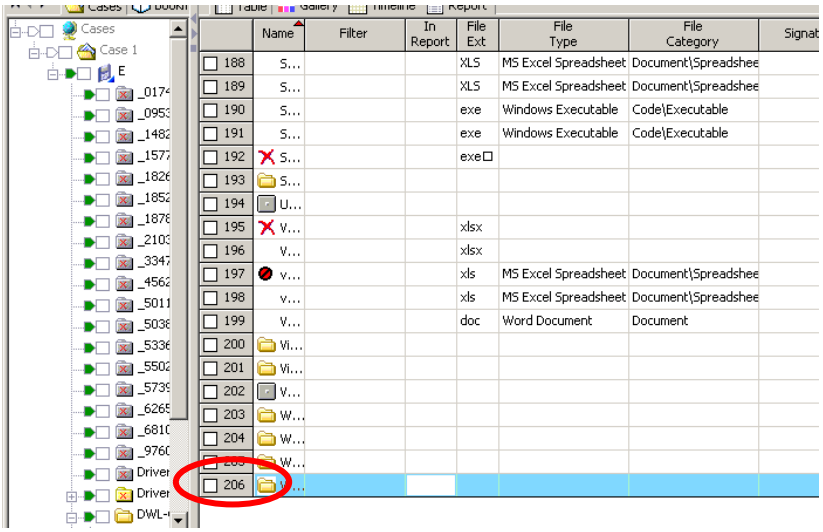
- Por lo general, en el slack space se encuentra información sobre las páginas web visitadas (por ejemplo, el webmail)

El dato informático
¿Cuántos datos informáticos en el disco duro?



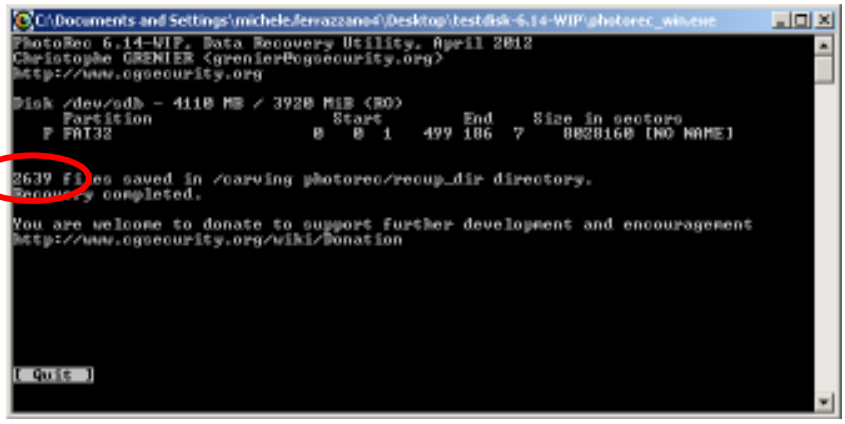
El dato informático

¿Cuántos datos informáticos en el disco duro?



El dato informático

¿Cuántos datos informáticos en el disco duro?



El dato informático

¿Cuántos datos informáticos en el disco duro?

- Archivos y carpetas visibles (in chiaro)
  - 137
- Archivos y carpetas eliminados
  - 206
- Archivos y carpetas recuperados
  - 2639

Copiad y subrayad en vuestros apuntes

- No se pueden obtener los datos informáticos con un simple "corta y pega"
  - Es reductivo
  - Puede dar lugar a alteraciones de datos
  - Puede dar lugar a equívocos
- Es necesario utilizar procedimientos de obtención de datos completos

El dato informático
Gestión de los archivos en un disco duro

- Además del espacio en el que físicamente se guardan los archivos, el disco duro mantiene un índice en el que se memoriza la posición en la que se guarda un archivo, así como otro tipo de información como
  - Nombre del archivo
  - Fecha y hora de creación
  - Fecha y hora de última modificación
  - Fecha y hora de última lectura
  - Si el archivo todavía es visible (in chiaro) o si ya ha sido cancelado
  - …

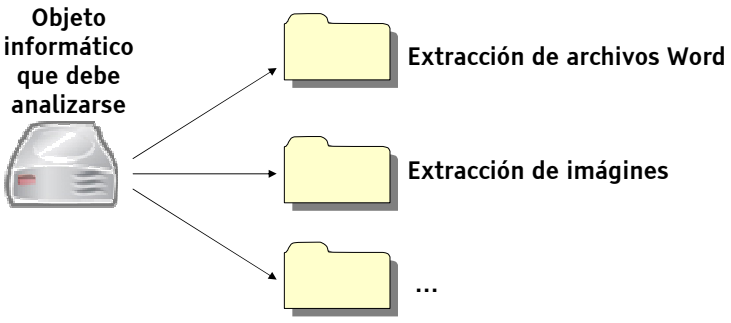
El dato informático

- Teniendo en cuenta la volatilidad del dato informático, es posible identificar 5 fases para su correcto tratamiento
  - Identificación
    - Los datos perdidos son irrecuperables
  - Obtención
    - Los datos maltratados son irrecuperables
  - Análisis
    - Actividad repetible: hace que surjan los datos relevantes
  - Valoración
    - Se transforma el “dato” en “información”
  - Presentación
    - Transmitir los resultados de la actividad a los juristas

Identificación

- ¡Debe ser exhaustiva!
- Se identifican todos los dispositivos que pueden contener datos digitales o digitalizados:
  - Ejs. Cámaras de video, teléfonos móviles, tabletas, micromemorias, automóviles, agendas electrónicas, electrodomésticos, fax, fotocopiadoras…

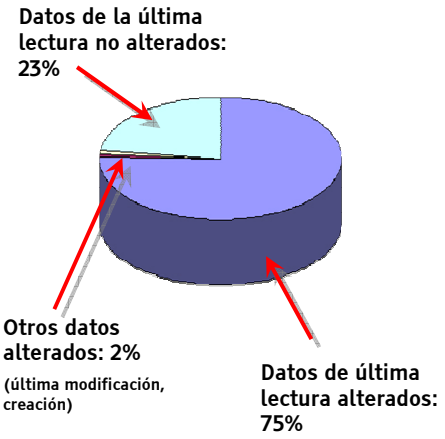
Acceso a los datos



Procedimiento incorrecto

Alteración de datos, identificación errónea

Accesso a los datos



- El acceso a los datos sin una protección adecuada puede dar lugar a una alteración masiva de datos
- Ejemplo
  - El empleo de la función "Buscar" de Windows modifica irreversiblemente todas las fechas de acceso a los archivos
  - Resulta imposible reconstruir los momentos de acceso a los archivos

Aseguramiento

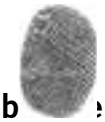
- Es reductivo limitarse solo a los archivos visibles (in chiaro)
  - Podríamos perder
    - Datos importantes presentes en el espacio eliminado
    - Metadatos
- Es necesario obtener todos los datos (todos los bits) presentes en el disco duro
- Copia bit-a-bit
  - Bit-stream image
  - Realización de más copias por motivos de seguridad
    - Al menos 2
    - Las *buenas prácticas* aconsejan al menos 3

Aseguramiento
La función Hash como instrumento de garantía

- En informática no existe diferencia entre original y copia
  - Son todos originales
- Al tiempo que se lleva a cabo la actividad de obtención, es preciso "marcar" de alguna manera el objeto informático, con el fin de verificar si se han producido alteraciones después de la adquisición
  - Función Hash

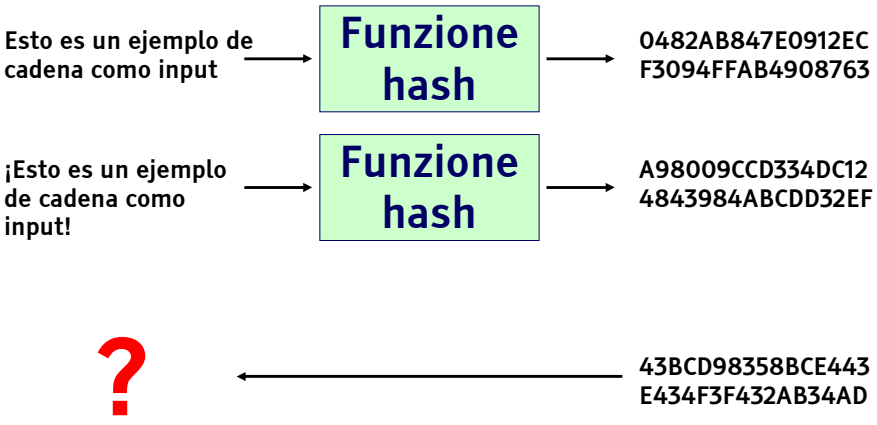
Aseguramiento
La función Hash como instrumento de garantía

- Conjunto de bits → Hash
- Ser humano → Huella digital

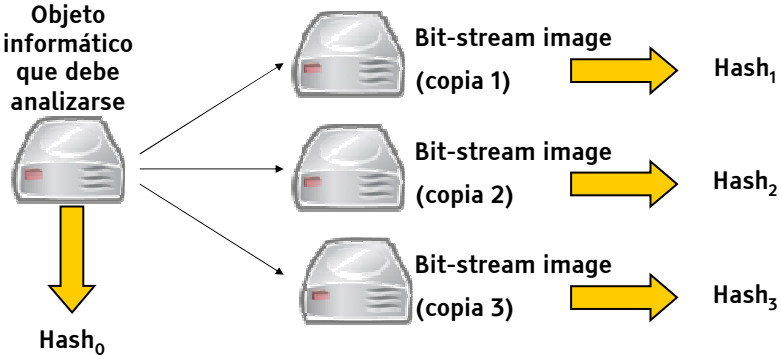


- Si se nos da como input un conjunto de b[illegible] cualquier longitud, la función hash produce como output una cadena de bits de tamaño fijo
  - La modificación de un solo bit del conjunto de bits de partida da lugar a una cadena de output completamente diferente
  - Si disponemos de una cadena de hash resulta imposible volver al conjunto de bits que la ha generado

Aseguramiento
La función Hash como instrumento de garantía



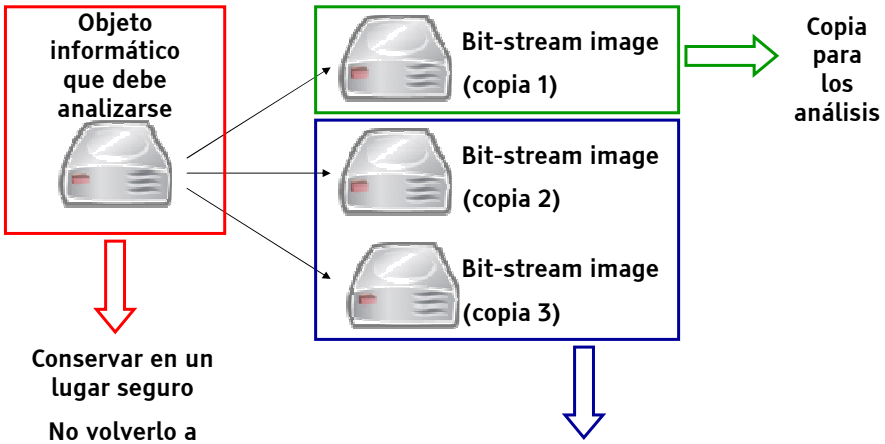
Aseguramiento
La función Hash como instrumento de garantía



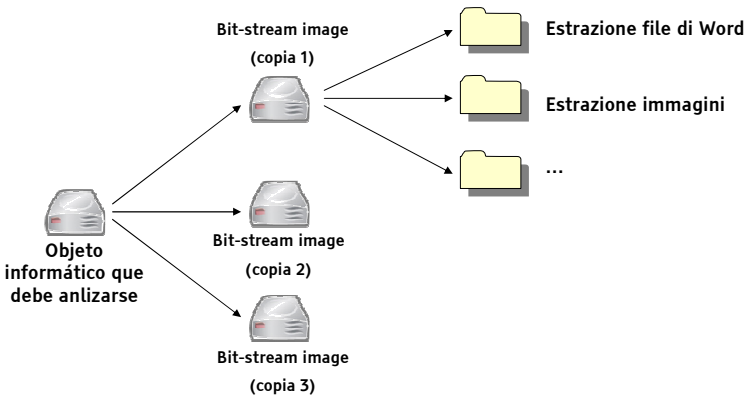
Requisitos que se deben cumplir

$Hash_0 = Hash_1 = Hash_2 = Hash_3$

Aseguramiento

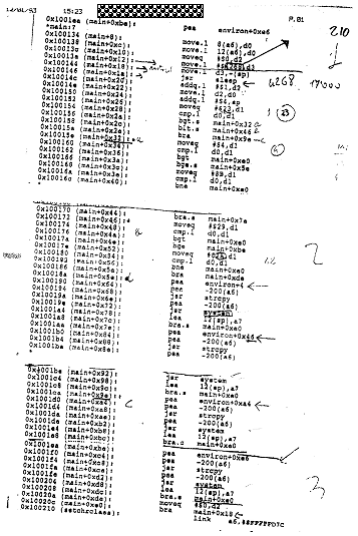


Aseguramiento



Procedimiento correcto

Aseguramiento



Aseguramiento

- El acceso al disco duro puede comportar la alteración de datos de forma automática
- Para prevenir, se debe usar un write blocker

Aseguramiento

Aseguramiento

Análisis

- Dado que cada copia coincide con el original, el análisis se practica sobre una copia de los datos obtenidos, y no sobre el original
  - Debe ser reproducible
  - Cada una de las operaciones practicada sobre los datos debe producir siempre el mismo resultado

Análisis

- Sobre la base del delito que se persigue y de los objetivos fijados, el análisis forense puede tomar distintas direcciones
  - Extraer los archivos del ordenador, incluso los cancelados
  - Comparar archivos de datos para conocer el contenido de los documentos y de los archivos de datos
  - Determinar el tiempo y la secuencia con los que los archivos de datos han sido creados, modificados o se ha accedido a ellos
  - Convertir el archivo de un formato a otro
  - Buscar por palabra clave entre los archivos de datos y en el espacio no ocupado
  - Recuperar contraseñas (cracking)
  - Analizar y comparar el código fuente [...]

Análisis

Veamos algunos ejemplos

1. Verificar la culpabilidad o la coartada de alguien investigado por homicidio
2. Descubrir las relaciones entre el investigado y otras personas
3. Verificar si el investigado ha descargado y divulgado material pedopornográfico
4. Verificar la correcta gestión financiera de una empresa

Análisis – Ejemplo 1

Verificar la culpabilidad o la coartada de alguien investigado por homicidio

- (En Italia) está de moda que el investigado por un homicidio esté escribiendo su trabajo de fin de carrera mientras se cometía un homicidio…

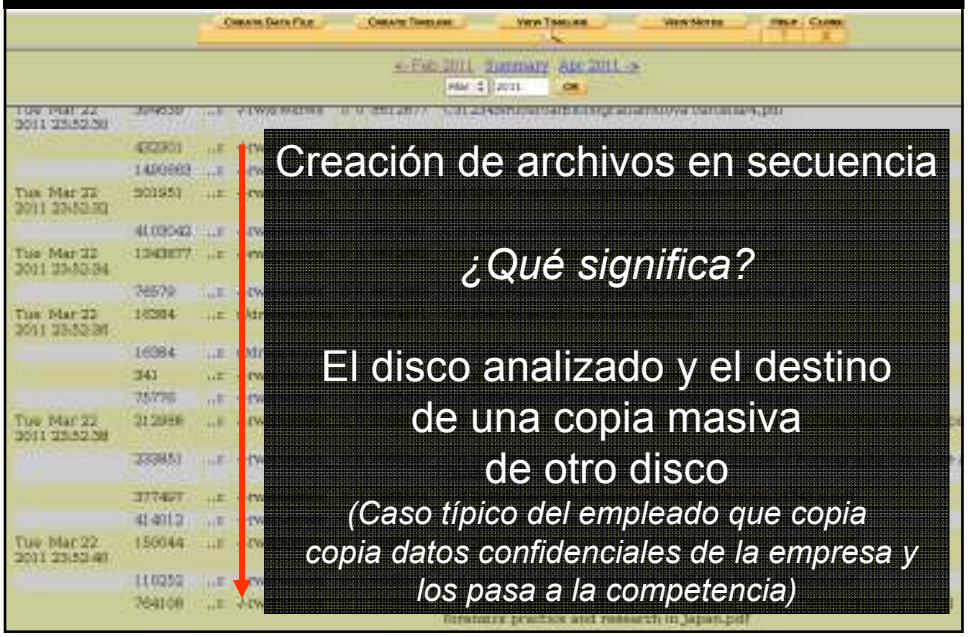
¿Cómo verificarlo?

- Análisis de la cronología
  - Acceso, modificación y creación de archivos
- Análisis de la interacción persona-ordenador
  - Navegación en Internet, envío de correo electrónico, chat
  - Redacción de documentos
  - Conexión de llaveros usb
  - …

Análisis – Ejemplo 1

- La cronología es una visualización sobre el horario de las operaciones de acceso, modificación y creación de archivos
  - Momentos en que se ha empleado el pc
  - Permite averiguar cuándo ha habido interacción persona y ordenador
  - Actividad de investigación o de copia masiva de archivos
  - Costumbres del usuario

Análisis – Ejemplo 1



Análisis – Ejemplo 2

Descubrir las relaciones entre el investigado y otras personas

¿Cómo verificarlo?

- Análisis de la navegación en Internet
- Análisis del correo electrónico (enviado y recibido)
- Análisis de las conversaciones de chat
- Análisis de los dispositivos móviles
  - Teléfonos móviles, smartphone, tabletas, navegadores GPS…
  - En particular: llamadas, SMS, MMS, Whatsapp, Viber, Skype, Gtalk, email, seguimiento de las células telefónicas, recorridos de la navegación…

Análisis – Ejemplo 3

Verificar si el investigado ha descargado y divulgado material pedopornográfico

¿Cómo verificarlo?

- Verificar la presencia de archivos pedopornográficos
- Verificar los instrumentos de intercambio de archivos
  - Intercambio de archivos P2P, email, acceso a sitios pedopornográficos…
- Se debe prestar atención a la cantidad de archivos que se han encontrado
  - Podría ser un archivo descargado por error o de forma inconsciente

Análisis – Ejemplo 4

Verificar la correcta gestión financiera de una empresa

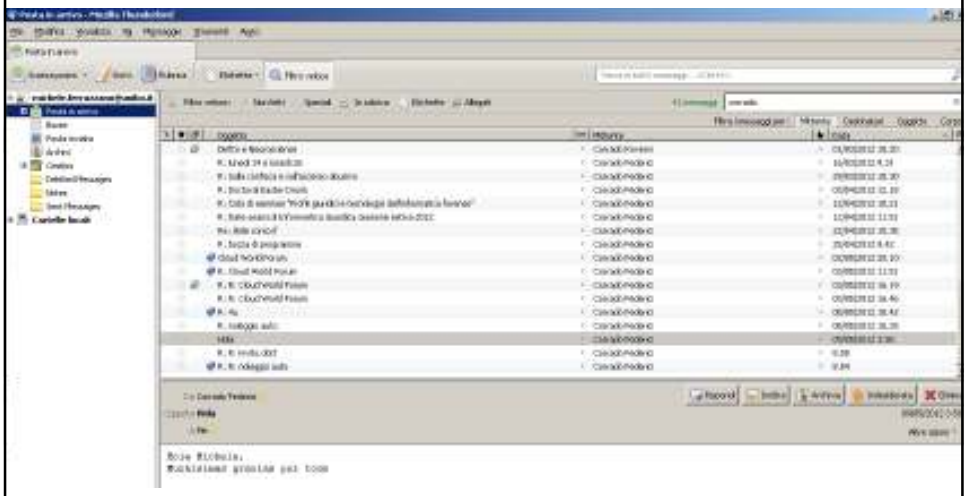
¿Cómo verificarlo?

- Análisis de los instrumentos de comunicación
  - Correo electrónico, SMS…
- Extraer y consultar todos los documentos
  - Documentos de Word, Excel, PDF…
- Verificar las fechas de la última modificación de los documentos
  - Y confrontarlas con los datos existentes en el backup para verificar eventuales manipulaciones

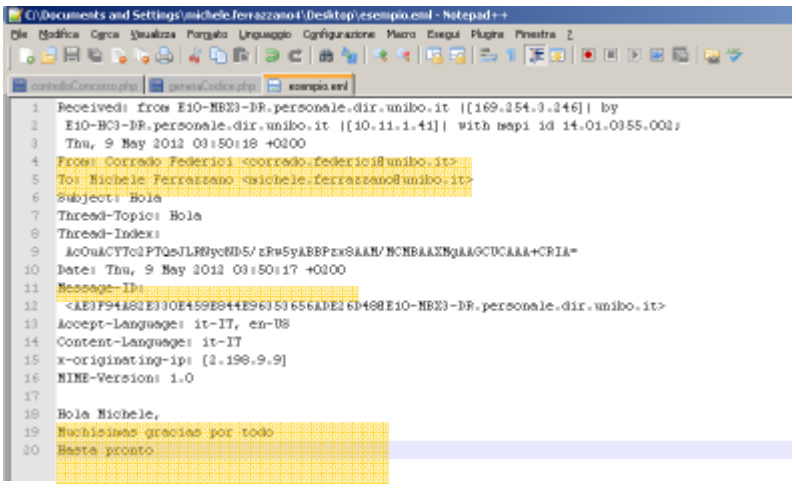
Análisis – El valor probatorio

- Se debe prestar atención a los documentos, especialmente si han sido presentados por el investigado (o por una de las partes, en una causa civile)
- Es extremadamente fácil crear documentos y correos electrónicos "ad arte", tanto por lo que se refiere al contenido como por lo relativo a los datos temporales
  - Fecha de envío de un e-mail, fecha de creación o modificación de un archivo
- Os lo demuestro…

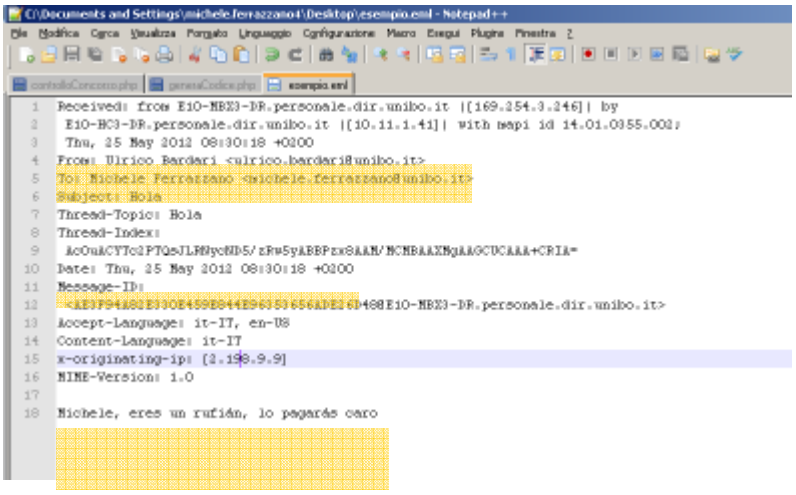
Análisis
El valor probatorio de un email



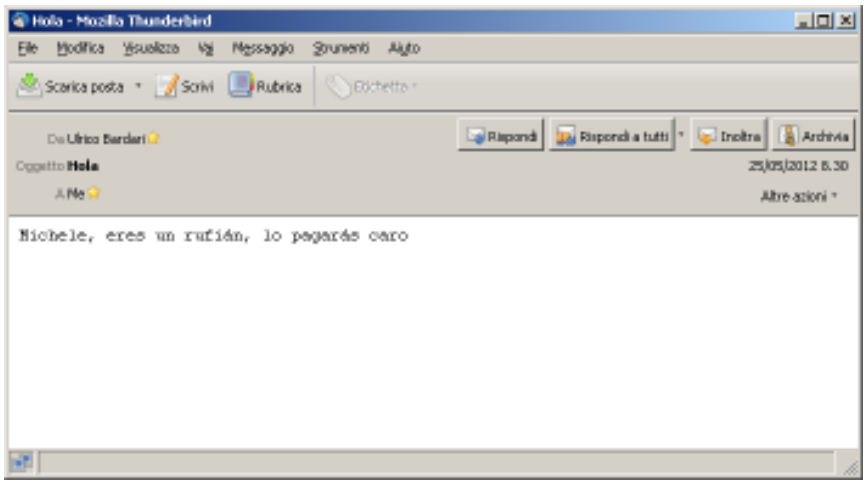
Análisis
El valor probatorio de un email



Análisis
El valor probatorio de un email



Análisis
El valor probatorio de un email



Valoración

- ¿Por qué es necesario evaluar el objeto informático si el bit solo puede tener como valor 0 ó 1?
- Porque dicho objeto puede ser fácilmente
  - Alterado
  - Contaminado
  - Falsificado
- En la fase de valoración es preciso
  - Verificar si las operaciones de obtención del objeto informático han sido legales
  - Expresar juicios de valor acerca de la atendibilidad, integridad y autenticidad del mismo objeto
  - Establecer la relación entre los datos que se han identificado

Valoración

Un ejemplo sencillo: infracciones en la circulación de vehículos a motor

Estimado Sr. Ferrazzano
Le informamos que en fecha 05/05/2005 el sistema automático de detección de infracciones en la circulación de vehículos a motor ha realizado la siguiente fotografía.
Por lo tanto, debe pagar una multa de € 100,00.
Adjunto se acompaña la impresión de la fotografía.

- Esto es un ejemplo de documento de constatación de una infracción semafórica efectuada por el coche blanco
- La prueba es una impresión de la fotografía
- Todas las fotografías realizadas por el aparato están en formato digital
  - Por lo tanto, son alterables
  - Una empresa privada se ocupa de imprimir las fotografías en las que se recogen las infracciones

Valoración

53

Un ejemplo sencillo: infracciones en la circulación de vehículos a motor

Valoración

54

Un ejemplo sencillo: infracciones en la circulación de vehículos a motor

La informática forense en las redes

- El contexto de disk forensics es más simple porque el objeto informático se recupera en un lugar físico preciso y puede ser custodiado más fácilmente
- En las redes es todavía más complicado
  - Y en la nube, todavía más
    - Sobre eso hablará Corrado Federici…

Preservación de una página web

Preservación de una página web

- Impresión de la página web

Preservación de una página web

O bien

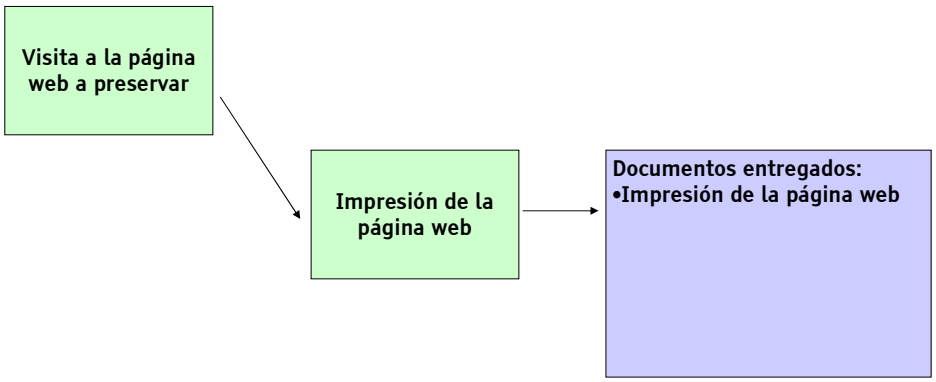
- Impresión de la página web auténtica por parte del notario

Preservación de una página web

- Pero ¡no es suficiente!
  - Se pierde muchísima información
  - Se limita a demostrar la percepción de quien visita el sitio, y no el origen ni la formación de los datos
  - La página podría haber sido alterada

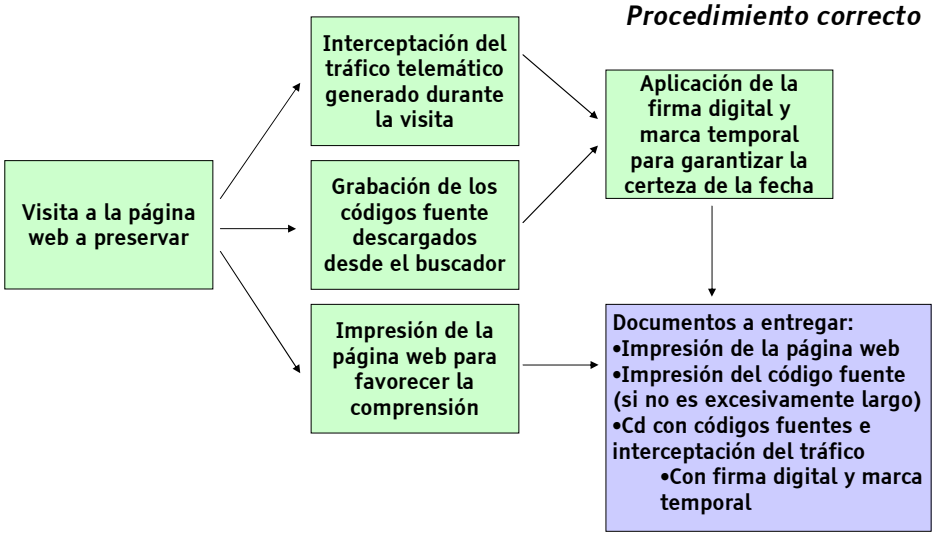
Preservación de una página web

Procedimiento incorrecto

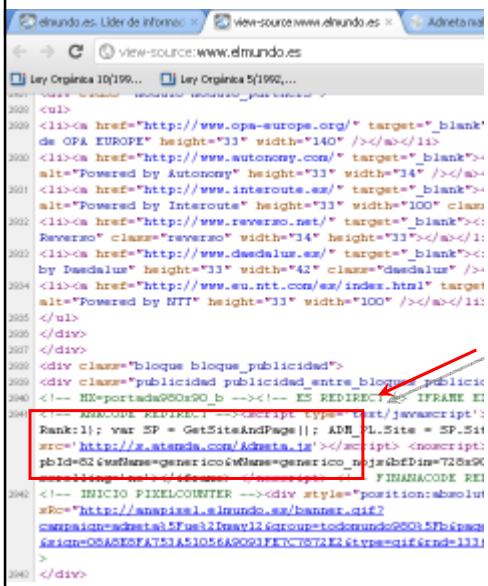


Preservación de una página web

Procedimiento correcto



Preservación de una página web

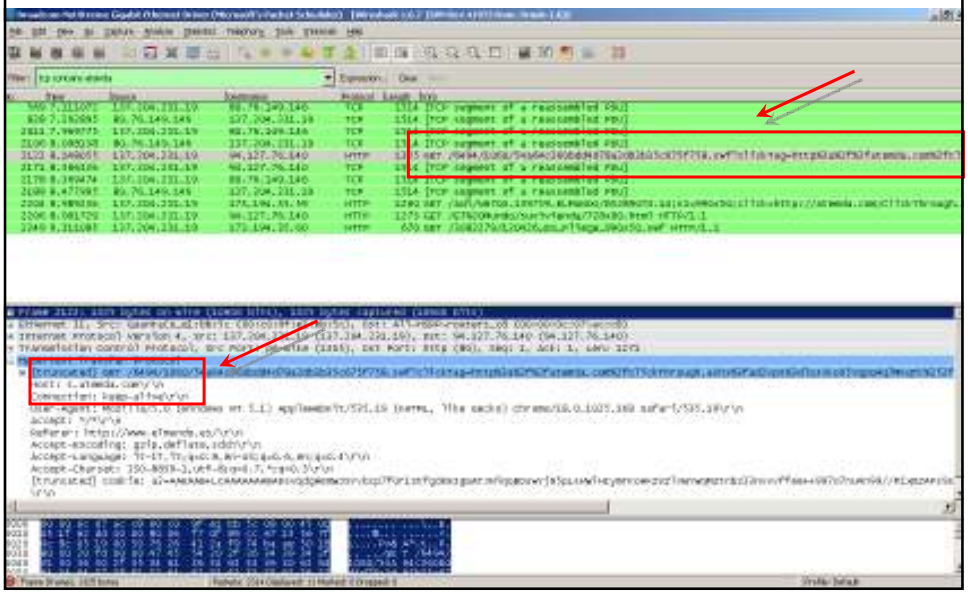


- Código fuente
- Permite entender de dónde viene la información
  - Por ejemplo, si en una página web aparecen imágines pedopornográficas, material protegido por derechos de autor, textos difamatorios... es importante entender quién ha colocado ese material
  - Los datos ilícitos podrían proceder de conexiones con otros sitios

Preservación de una página web

- Este trozo de fuente procede de otro sitio
- Si el administrador de este sitio cambiase el código, la página que lo uso se encontraría con efectos indeseados y por sorpresa

Preservación de una página web



Conclusiones

- Hagamos un resumen de lo dicho hasta ahora
- Valoremos los costes y los beneficios de la informática forense

Investigación informática
Problemas

- Necesidad de conocimiento/método científico
- Ausencia de sistematicidad en los métodos empleados por los investigadores
- Falta de estandards aceptados a nivel nacional e internacional tanto para la práctica como por la formación
  - Necesidad de invertir en el aspecto formativo y profesionalizador del *computer forensics expert*

Investigación informática
Correcto tratamiento del dato informático

- Conservación, no alteración y garantía de inmodificabilidad
  - Es fácil alterar el dato informático (incluso de forma involuntaria)
  - Puede ser difícil encontrar pistas sobre los autores de la alteración
  - Se pueden perder datos importantes para siempre
- Sello electrónico
  - Empleo de instrumentos de memorización y de técnicas que garanticen lo dicho supra
    - Soportes ópticos, firma digital, marca temporal

Problemas en la investigación informática
Algunas soluciones

- Metodologías científicas de recogida, análisis y gestión de las pruebas informáticas
  - Preservar el dato informático
- Formación específica para los operadores procesales (magistrados, policía judicial, abogados, técnicos, operadores forenses)
- Ósmosi entre el mundo técnico-informático y el mundo jurídico

¿Cuánto cuesta?
Pensemos al nivel de una oficina

- Preservación
  - Realización de una copia forense usando el ordenador del investigado y una distribución forense
    - Aproximadamente 100€
      - Coste de dos discos duros para salvar los datos
  - Realización la copia forense de un teléfono móvil
    - X €
      - Coste de los DVD para grabar los datos
    - X.XXX € (una tantum)
      - Coste de los aparatos y de todos los cables para los móviles
        - Ejemplo: Cellebrite UFED 4000$

¿Cuánto cuesta?
Pensemos al nivel de una oficina

- Análisis
  - Utilizzndo software comercial
    - X.XXX € - XX.XXX€
  - Utilizando software open source
    - 0 €
  - Algunos software comerciales ofrecen muchas prestaciones y no hay alternativas opensource

¿Cuánto cuesta? Pensemos al nivel de una oficina

- ¿Cual es el coste principal?

  LA FORMACIÓN DEL PERSONAL

- Motivos
  - Infravaloración del problema
  - Falta de tiempo

- Si se invierte en formación del peronal (uso de los sistemas informáticos, pero, sobre todo, metodología y rigor científico) se puede ahorrar mucho dinero en peritajes externos, al tiempo que se prestan mayores garantías a las partes

Fin

Gracias por la atención

Michele Ferrazzano
michele@informaticaforense.it