

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 ambientes ligados al common law y con un alto grado de evolución tecnológica, como los EEUU
- Existen agencias especializadas que certifican
 - software
 - hardwareempleado 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

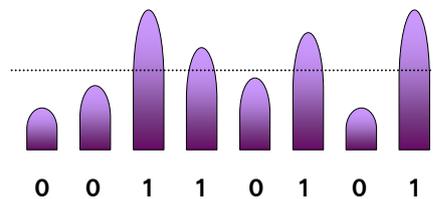
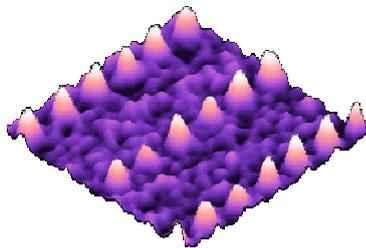
El dato informático

- 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

5

- El bit es intangible
- 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



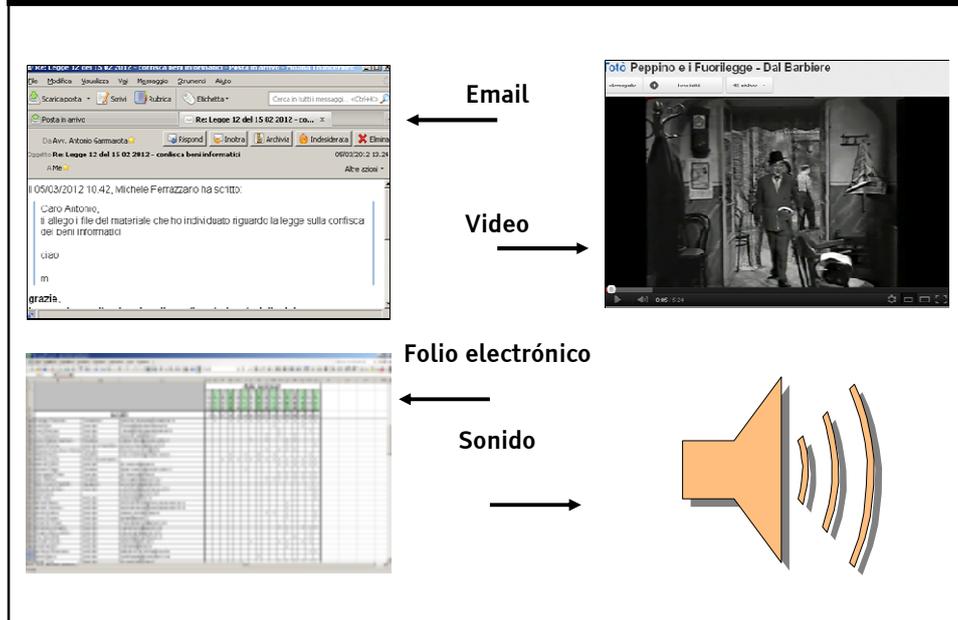
El dato informático

6

- 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, impidiendo 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)

7



El dato informático

8

- ¿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

9

Gestión de los archivos en un disco duro

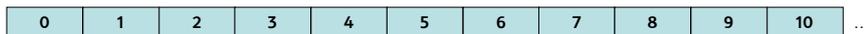
- Un disco duro está organizado de forma lógica mediante el uso de un sistema de archivos
 - El sistema de archivos divide el espacio disponible en el disco duro en sectores de iguales dimensiones
 - Cuando se graba un archivo, se usa el menor número posible de sectores, pero siempre en número suficiente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

El dato informático

10

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

11

Nombre archivo	Dónde empieza	Existe?
Seminario.doc	1	Si

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

El dato informático Gestión de los archivos en un disco duro

12

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

1	La prueba informa
2	tica: instrumentos
3	y metodología 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

13

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

14

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

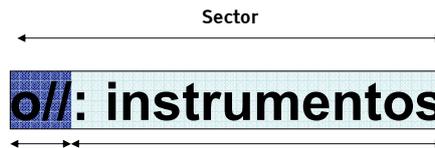
1	Michele Ferrazzan
2	o//: instrumentos
3	y metodologia rela
4	tivos al analisis fo
5	rense de discos du
6	ros y de redes//
7	Seminario de info
8	rmatica forense//
9	
10	
11	
12	

El dato informático

Gestión de los archivos en un disco duro

15

- Algunos datos pueden sobrevivir durante años en el slack space



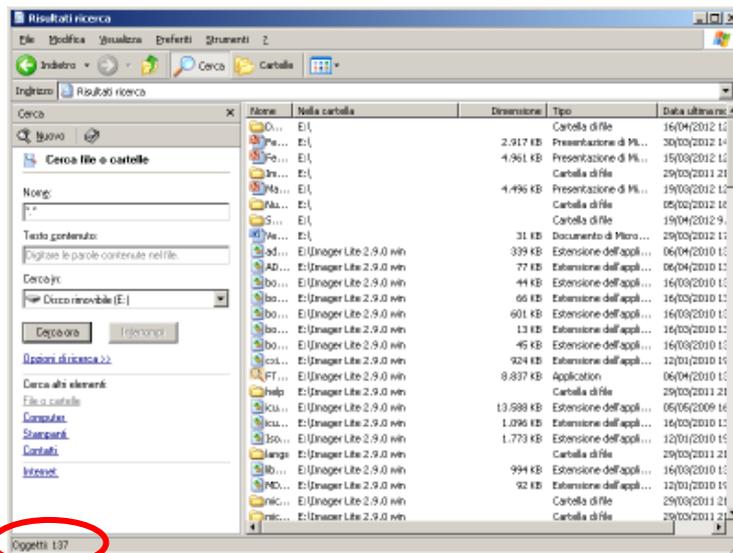
Espacio ocupado por el archivo SLACK SPACE

- 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?

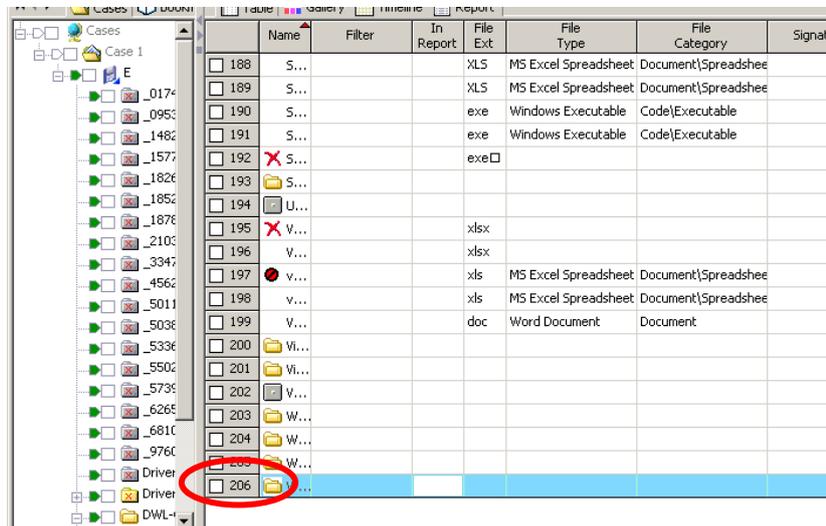
16



El dato informático

17

¿Cuántos datos informáticos en el disco duro?



	Name	Filter	In Report	File Ext	File Type	File Category	Signat
<input type="checkbox"/>	188	S...		XLS	MS Excel Spreadsheet	Document\Spreadshee	
<input type="checkbox"/>	189	S...		XLS	MS Excel Spreadsheet	Document\Spreadshee	
<input type="checkbox"/>	190	S...		exe	Windows Executable	Code\Executable	
<input type="checkbox"/>	191	S...		exe	Windows Executable	Code\Executable	
<input type="checkbox"/>	192	X S...		exe			
<input type="checkbox"/>	193	S...					
<input type="checkbox"/>	194	U...					
<input type="checkbox"/>	195	X V...		xlsx			
<input type="checkbox"/>	196	V...		xlsx			
<input type="checkbox"/>	197	v...		xls	MS Excel Spreadsheet	Document\Spreadshee	
<input type="checkbox"/>	198	v...		xls	MS Excel Spreadsheet	Document\Spreadshee	
<input type="checkbox"/>	199	V...		doc	Word Document	Document	
<input type="checkbox"/>	200	V...					
<input type="checkbox"/>	201	Vi...					
<input type="checkbox"/>	202	V...					
<input type="checkbox"/>	203	W...					
<input type="checkbox"/>	204	W...					
<input type="checkbox"/>	205	W...					
<input type="checkbox"/>	206						

El dato informático

18

¿Cuántos datos informáticos en el disco duro?

```
C:\Documents and Settings\michele.ferrazzano\Desktop\test@isk-6.14-WIP\ghaterec_wipeout
PhotoRec 6.14-WIP, Data Recovery Utility, April 2012
Christophe GRENIER <grenier@ogosecurity.org>
http://www.ogosecurity.org

Disk /dev/sdb - 4118 MB / 3928 MiB (RO)
Partition      Start          End      Size in sectors
F FAT32        B 0 1 499 186 7  8828160 [NO NAME]

2639 files saved in /carving/photorec/recup_dir directory.
Recovery completed.

You are welcome to donate to support further development and encouragement
http://www.ogosecurity.org/wiki/donation

[ Quit ]
```

El dato informático

19

¿Cuántos datos informáticos en el disco duro?

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

El dato informático

20

¿Cuántos datos informáticos en el disco duro?

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

21

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

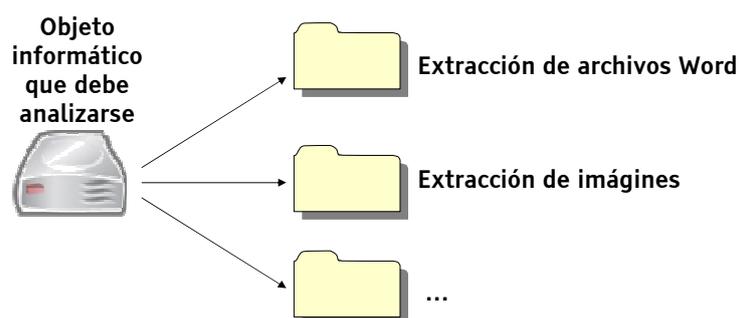
22

- 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

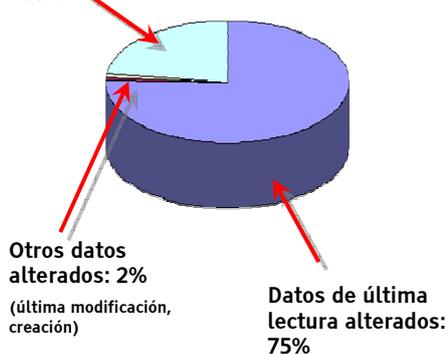


Procedimiento incorrecto

Alteración de datos, identificación errónea

Acceso a los datos

Datos de la última lectura no alterados: 23%



- 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 claro)
 - 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

27

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

28

La función Hash como instrumento de garantía

- Conjunto de bits → Hash
- Ser humano → Huella digital 
- Si se nos da como input un conjunto de bits de 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

29

La función Hash como instrumento de garantía

Esto es un ejemplo de cadena como input

Funcione hash

0482AB847E0912EC
F3094FFAB4908763

¡Esto es un ejemplo de cadena como input!

Funcione hash

A98009CCD334DC12
4843984ABCDD32EF

?

43BCD98358BCE443
E434F3F432AB34AD

Aseguramiento

30

La función Hash como instrumento de garantía

Objeto informático que debe analizarse



Hash₀



Bit-stream image (copia 1)

Hash₁



Bit-stream image (copia 2)

Hash₂



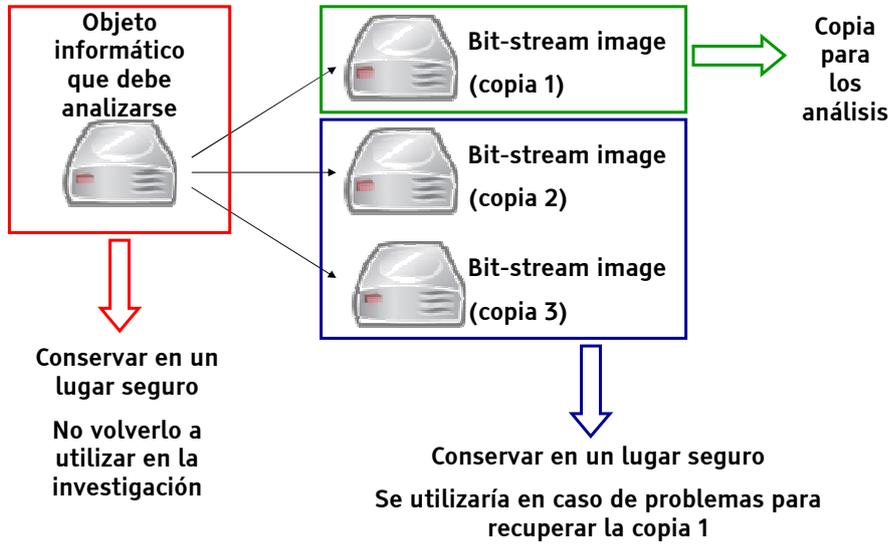
Bit-stream image (copia 3)

Hash₃

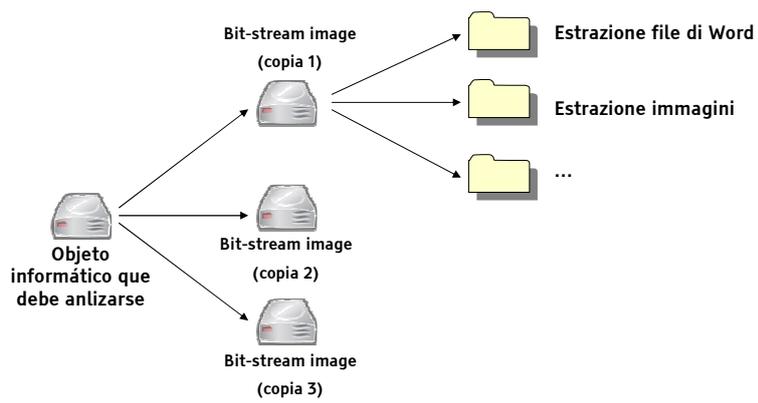
Requisitos que se deben cumplir

$$\text{Hash}_0 = \text{Hash}_1 = \text{Hash}_2 = \text{Hash}_3$$

Aseguramiento



Aseguramiento



Procedimiento correcto

Aseguramiento

35



Aseguramiento

36

MD5: 768bceb5a482e6
a4385777d2ee86b482 #

hash.txt
Messaggio MIME PKCS #7
5 KB

Dati sulla Firma								
Numero File	Dato Verifica	Algoritmo Digest	Firmatario	Dato Certificatore	Cod. Fiscale	Stato	D	
1	hash.txt.p7m (Firma totali apposta: 2)	Firma CADES OK	SHA-256	MICHELE PERRAZZANO	InfoCert Firma Qualificata	FRR99L86A0306-04W	IT	NC
2	Firma sulla Firma OK Data/Marca: 03/05/2011 22:44:01 (UTC Time)	SHA-256	3CED7922201304	InfoCert Time Stamping Authority			IT	LI

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 [...]

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

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...

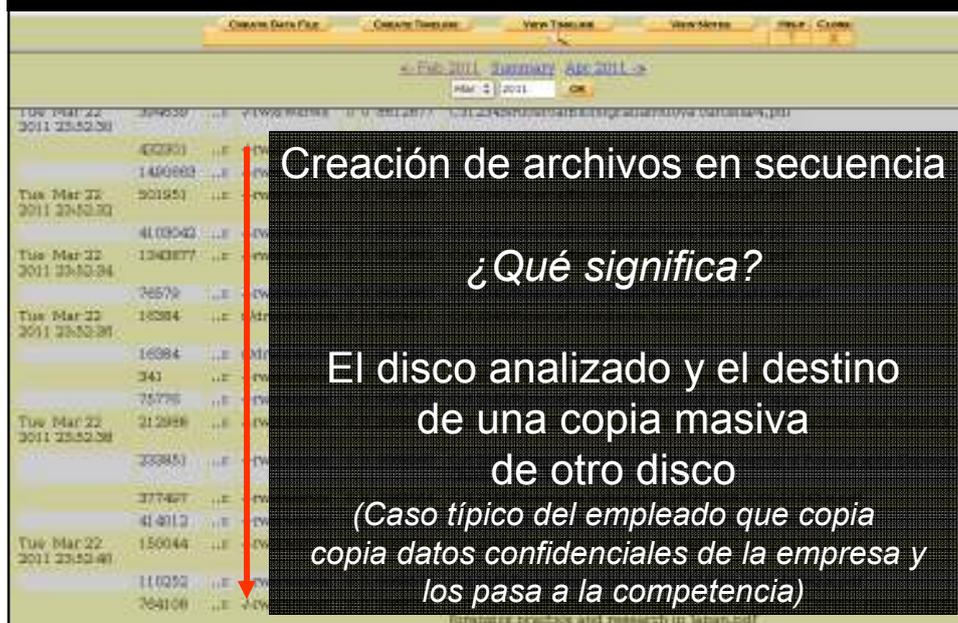
¿Cómo verificarlo?

- 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

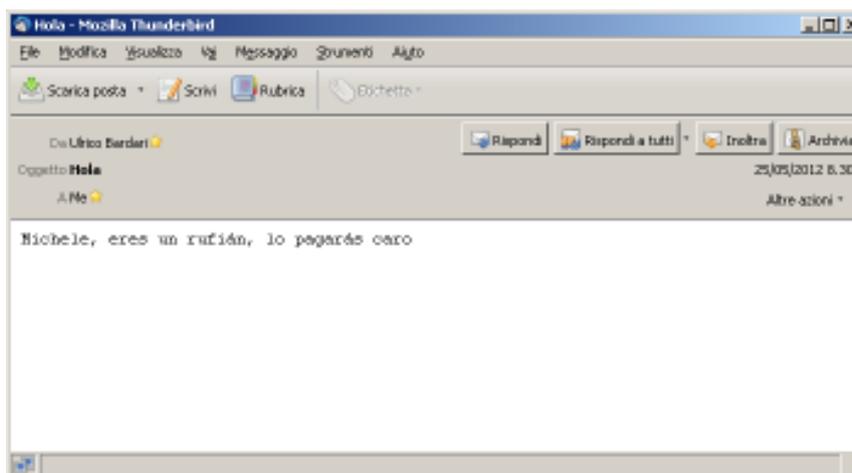
Análisis – El valor probatorio

- Se debe prestar atención a los documentos, especialmente si han sido presentados por el investigado (o por una de las partes, en una causa civil)
- 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

```
C:\Documents and Settings\michele.ferrazzano\Desktop\esempio.eml - Notepad++
File Modifica Cerca Visualizza Formato Linguaggio Configurazione Macro Eseguí Plugins Finestra ?
contenutoConcorso.php | generaCodice.php | esempio.eml
1 Received: from E10-MB23-PR.personale.dir.unibo.it ([169.254.3.246]) by
2 E10-MC3-PR.personale.dir.unibo.it ([10.11.1.41]) with mapi id 14.01.0955.002
3 Thu, 25 May 2012 08:30:18 +0200
4 From: Uirico Bardari <uirico.bardari@unibo.it>
5 To: Michele Ferrazzano <michele.ferrazzano@unibo.it>
6 Subject: Hola
7 Thread-Topic: Hola
8 Thread-Index:
9 AoOuACTYtoPTQsJLWBycND5/zW5yABBPz8AAK/NCHBAAXNqAAOCUAAA+CRIA=
10 Date: Thu, 25 May 2012 08:30:18 +0200
11 Message-ID:
12 <AED794480E330E4598844E94353456ADE261468E10-MB23-PR.personale.dir.unibo.it>
13 Accept-Language: it-IT, en-US
14 Content-Language: it-IT
15 x-originating-ip: [2.198.9.9]
16 MIME-Version: 1.0
17
18 Michele, eres un rufián, lo pagarás caro
19
```

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

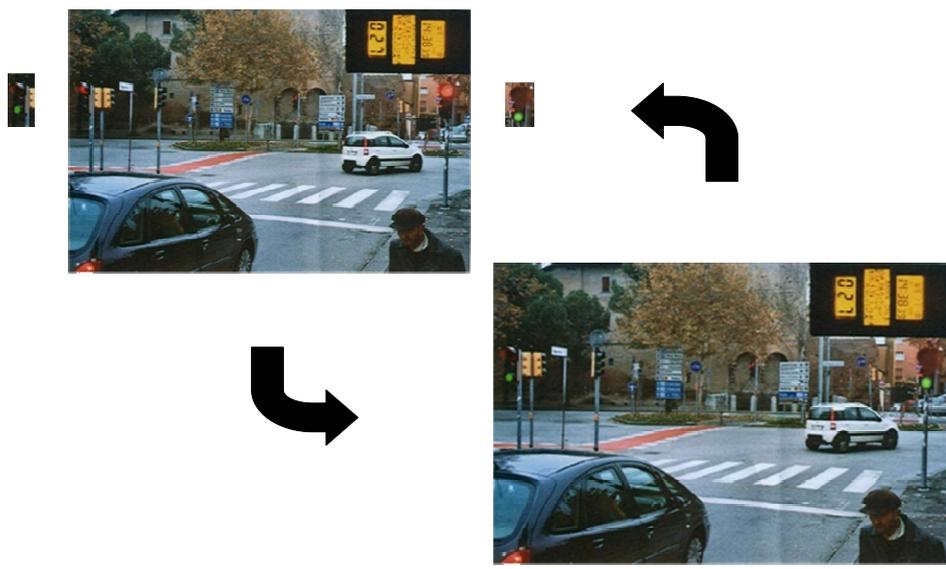
Un ejemplo sencillo: infracciones en la circulación de vehículos a motor



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

The image shows a screenshot of the El Mundo website. The main content area features a large advertisement for a Volkswagen Passat, with the text "ES UN PASSAT CON 4 AÑOS DE MANTENIMIENTO POR 22.800 €" and "2.500 € DE AYUDA POR 0,00000 €". Below the advertisement, there is a news article titled "Rajoy, dispuesto a salvar bancos con dinero público" with a sub-headline "El Gobierno pondrá 7.000 millones para sanear Bankia". The article text includes: "El presidente del Gobierno se agacha con el 'no' de los bancos como se agachó en los meses anteriores tras de haber optado por no hacer ni un centavo para salvar los gigantes? Ha afirmado que no es posible de otro lado, ha dicho: 'El Gobierno pondrá 7.000 millones para sanear Bankia'. También: 'Espero a los bancos para que se comprometan a devolver el 10%'". To the right of the article, there is a financial widget for "openbank" showing a "Cuenta nueva con 3,00% TAE" and a balance of "6.940,200" with a change of "+0,55% (+1,2)". At the bottom, there is a section for "MIRÓ" with the headline "Hollande busca un 'nuevo punto de partida'" and a large number "57". The website has a green sidebar on the left and right with the text "Lea 15 días GRATIS".

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

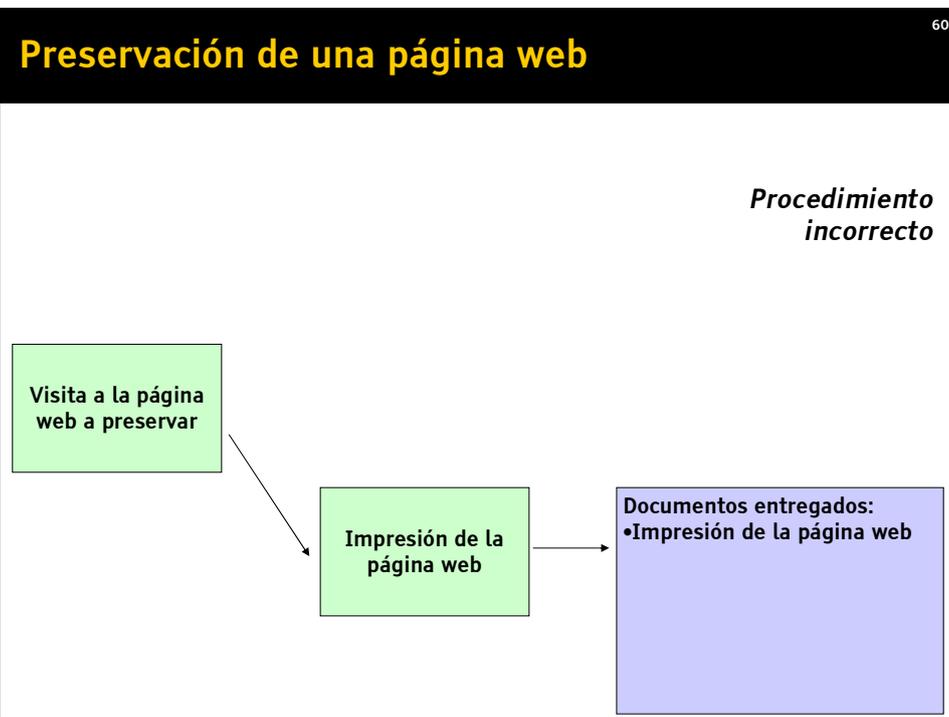
Preservación de una página web

Procedimiento incorrecto

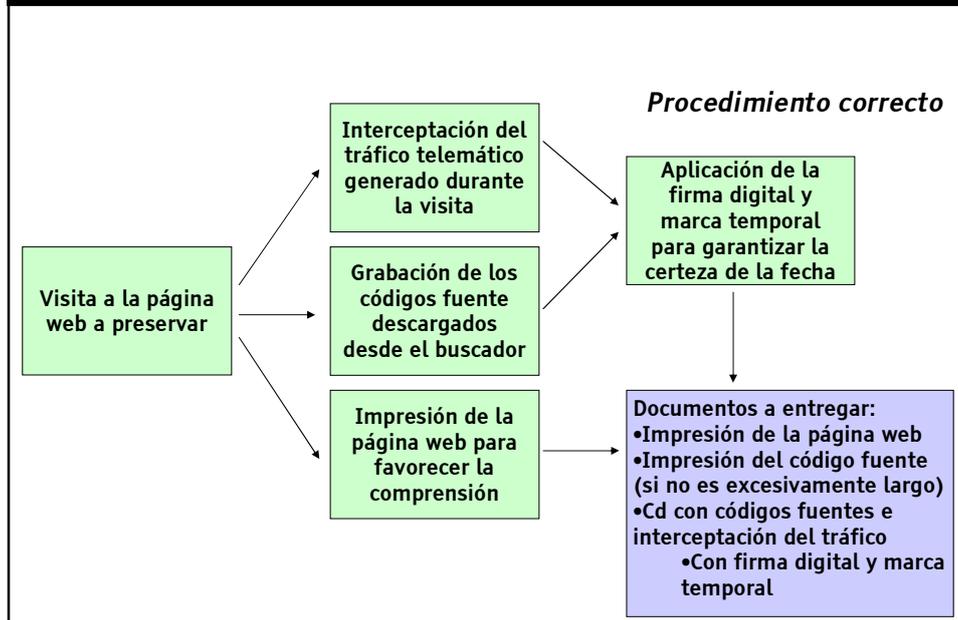
Visita a la página web a preservar

Impresión de la página web

Documentos entregados:
• Impresión de la página web



Preservación de una página web



Preservación de una página web

```

Rank:1; var SP = GetSiteAndPage(); ADM = L.Site = SP.Site;
src="http://g_atanda.com/Adستا.ig"></script> <noscript>
pbId=82 &#Name=generico&#Name=generico_njsgbDir=72&#K
</div>
  
```

- Código fuente
- Permite entender de dónde viene la información
 - Por ejemplo, si en una página web aparecen imágenes 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

```

// Copyright (c) Adbeta AB 2008-2012
// Version 1.56

var Adbeta=Adbeta||{};

Adbeta.version="1.56";
Adbeta.textVersion="2.19";
if(!Adbeta.base) Adbeta.base="http://atenda.com/";
if(!Adbeta.textAdsJS) Adbeta.textAdsJS="http://s.atenda.com/script/TextAd
Adbeta.singleImpression="JS&dservingSP.ashx?wId={wId} spId={pId} crank={cr
(wId) svit={vit} sjcob={jacob}";
Adbeta.singleImpressionBlended="JS&dservingSP.ashx?pbId={pbId} suelase={suel
(ems) sjcov={jcov} stov={tov} sob={obi} sFl={fL} svitp={witp} svit={vit} sjcob={joc
Adbeta.pageImpression="JS&dservingMP.ashx?po={po} spId={pId} solk={olk} se
(jacob)";
Adbeta.pageRepeatParam="spId={pId} crank={crank} sgId={gId} solk={olk}";
Adbeta.pageRepeatParamBlended="suelase={suelase} suelase={suelase} crank={o
if(!Adbeta.focus) Adbeta.focus=1;

Adbeta.init = function (vtUrl)
{
    if(Adbeta.initialized) return;

    Adbeta.SIV.init(vtUrl);

    if (window.addEventListener) {
        window.addEventListener("focus", Adbeta.onFocus, false);
        window.addEventListener("blur", Adbeta.onBlur, false);
    }
    else if (window.attachEvent) {

```

- 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

The screenshot shows the browser's developer tools with the Network tab selected. A request to `s.atenda.com/js/TextAd.js` is highlighted in green. A red box surrounds the request URL and the 'Referer' header, with red arrows pointing to them. The 'Referer' header is `http://www.atenda.es/vn`. The headers section shows various request details, including the user agent and accept headers.

Conclusiones

65

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

Investigación informática

66

Problemas

- Necesidad de conocimiento/método científico
- Ausencia de sistematicidad en los métodos empleados por los investigadores
- Falta de standards 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

67

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

68

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?

69

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?

70

Pensemos al nivel de una oficina

- **Análisis**
 - Utilizndo 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

71

- ¿Cual es el coste principal?
LA FORMACIÓN DEL PERSONAL
- Motivos
 - Infravaloración del problema
 - Falta de tiempo
- Si se invierte en formación del personal (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

72

Gracias por la atención

Michele Ferrazzano
michele@informicaforense.it