

# A2.2. Parte 1 - Análisis forense del sistema informático

Imagen Presentación  
Imagen Presentación

**Fecha:** 13 de enero de 2026

**Autor:** Sergio González

---

## Índice

1. **Introducción**
2. **Entorno de trabajo**
3. **Análisis del sistema operativo**
4. **Análisis de usuarios del sistema**
5. **Análisis de evidencias digitales**
6. **Conclusión**

---

### **## 1. Introducción**

---

#### **## 2. Entorno de trabajo**

El análisis forense se ha realizado en un equipo local con **Windows 11** como sistema operativo. Para examinar la evidencia digital se ha utilizado principalmente **Autopsy**, una herramienta forense ampliamente empleada para el análisis de imágenes de disco y recuperación de información.

La evidencia recibida consiste en un archivo comprimido que contiene cuatro volúmenes de imagen forense en formato **E01**: AFI\_W.E01, AFI\_W.E02, AFI\_W.E03 y AFI\_W.E04. Estos archivos se cargarán en Autopsy para llevar a cabo la exploración y extracción de hallazgos, respetando en todo

---

## ## 1. *Introducción*

---

momento la integridad de la evidencia.

### ### Descarga e instalación de Autopsy

Autopsy se descargó desde la página oficial ([autopsy.com](http://autopsy.com)) y se instaló siguiendo los pasos estándar para Windows. Esta herramienta permite crear casos forenses, cargar imágenes de disco y explorar sus contenidos de manera segura y controlada.

image

### ### Preparación del caso y carga de la imagen

Se creó un **nuevo caso** en Autopsy con el nombre “Drug Trafficking”. A continuación, se cargó el primer volumen de la imagen forense en formato **E01** (AFI\_W.E01), que incluye automáticamente los demás volúmenes (AFI\_W.E02, AFI\_W.E03 y AFI\_W.E04). Autopsy verificó la integridad de la imagen completa al momento de cargarla y generó un árbol de archivos listo para su análisis.

image

### ### Verificación de integridad de la evidencia

Se recibieron cuatro volúmenes de imagen forense (AFI\_W.E01 a AFI\_W.E04) junto con sus respectivos hashes de adquisición proporcionados en un PDF:

image

Los archivos descargados localmente tienen los siguientes hashes calculados:

#### - **AFI\_W.E01:**

bash

28FE02881E6AFE82B2CE74249CA0CF33

image

#### - **AFI\_W.E02:**

---

## ## 1. Introducción

---

bash

07A4E96473DD0163F68C87CE9C9C1F22

image

- **AFI\_W.E03:**

bash

FE1578A3D67F1C55ADA968E86B995590

image

- **AFI\_W.E04:**

bash

C4C8AFB97E19EDBD0CA47B3DAC33E94E

image

-

**Evidencias\_Drug\_Trafficking.zip:**

bash

8C74E07D868ACF37B53FB75CEFAF20E5

image

Al comparar ambos conjuntos de valores, se confirma que **todos los archivos coinciden exactamente con los proporcionados**, lo que garantiza que la evidencia está íntegra y no ha sido alterada desde su adquisición.

---

## 3. Análisis del sistema operativo

A continuación se responde a las preguntas relacionadas con el sistema operativo instalado en la imagen forense analizada, utilizando la información obtenida mediante la herramienta Autopsy.

**¿Qué tamaño tiene la partición a analizar?**

La partición analizada tiene un tamaño de **2.623.832.064 bytes**, lo que equivale aproximadamente a **2,45 GB**.

image

**Sistema y versión del sistema operativo instalado**

El sistema operativo identificado es **Microsoft Windows XP Service Pack 3 (x86)**.

image

## **Nombre del usuario y organización registrados**

- **Usuario registrado (Owner):** john

- **Organización registrada:** home

image

## **“Product ID” asociado al sistema**

El *Product ID* asociado al sistema operativo es

**76487-341-1072684-22504.**

image

## **“Service Pack” instalado**

El sistema tiene instalado **Service Pack 3**, correspondiente a Windows XP.

image

## **Fecha y hora de instalación del sistema operativo**

La fecha y hora de instalación del sistema operativo es

**23/04/2013 a las 02:07:59 (CEST).**

image

## **Fecha y hora del último “shutdown”**

El último apagado registrado del sistema tuvo lugar el

**25/04/2013 a las 04:06:34 (CEST).**

image

---

### **## 4.**

#### ***Análisis de usuarios del sistema***

---

###

Usuario:

john

- **Último**

**logon:**

28/03/2013

04:10:49

CET -

**Último**

**cambio de**

**contraseña:**

No

disponible /

Contraseña

no expira

image

---

### Usuario: ian

- **Último logon:** 25/04/2013 04:06:52 CET
- **Último cambio de contraseña:** No disponible / Contraseña no expira

image

---

### Usuario: jessy

- **Último logon:** 23/04/2013 04:18:56 CET
- **Último cambio de contraseña:** No disponible / Contraseña no expira

image

---

### Usuario: support\_388945a0

- **Último logon:** No disponible (Cuenta de servicio de soporte, 0 logins)
- **Último cambio de contraseña:** No disponible / Contraseña no expira

image

---

### Usuario: helpassistant

- **Último logon:** No disponible (Cuenta Remote Desktop Help Assistant, 0 logins)
- **Último cambio de contraseña:** No disponible / Contraseña no expira

image

### Observaciones

- Los usuarios **john**, **ian** y **jessy** sí se han logueado y las fechas tienen sentido con la actividad del sistema.
- Las cuentas **support\_388945a0** y **helpassistant** son cuentas de sistema, no han iniciado sesión nunca, así que no hay logons que mostrar.
- Ninguno de los usuarios tiene fecha de cambio de contraseña porque todas las cuentas están configuradas para **que la contraseña no caduque**.

---

## **## 5. Análisis de evidencias digitales**

---

**###**  
Archivos  
eliminados

---

### **1. fabricando coca 4.jpg**

- **Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/fabricando coca 4.jpg
- **Tamaño:** 12.608 bytes
- **MAC Times:**
  - Creación: 2013-06-19 04:11:24 CEST
  - Modificación: 2013-03-27 06:43:30 CET
  - Último acceso: 2013-06-19 04:11:24 CEST
- **Hash MD5:** ffbedbaa75fff0a2f405489082667c65
- **Hash SHA-256:**  
7c6dffced23041315aa7fb9e3ac90e2f3934e1430d819eebb135e  
e9d634c3b63
- **Tipo:** image/jpeg

image

---

**#### 2. fabricando coca 3.jpg - Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/fabricando coca 3.jpg - **Tamaño:** 9.994 bytes - **MAC Times:** - **Creación:** 2013-06-19 04:11:24 CEST - **Modificación:** 2013-03-27 06:43:20 CET - **Último acceso:** 2013-06-19 04:11:24 CEST - **Hash MD5:** 99631163aabed753f9a5d00b6fe74ac - **Hash SHA-256:** 800242322a228a4db8567b0de03f33f259ebd46e6601b51a2b8e4907f7c87 - **Tipo:** image/jpeg

---

**#### 3. fabricando coca 2.jpg - Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/fabricando coca 2.jpg - **Tamaño:** 14.373 bytes - **MAC Times:** - **Creación:** 2013-06-19 04:11:24 CEST - **Modificación:** 2013-03-27 06:42:34 CET - **Último acceso:** 2013-06-19 04:11:24 CEST - **Hash MD5:** 5131b40b7b745677b6a6b06e3580508c - **Hash SHA-256:** 12ac6ae66c460ba004e1389991f429495246d743080c2c00c05c326b4da8368c - **Tipo:** image/jpeg

image

---

### **4. fabricando coca.jpg**

- **Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/fabricando coca.jpg
- **Tamaño:** 6.413 bytes
- **MAC Times:**
  - Creación: 2013-06-19 04:11:24 CEST
  - Modificación: 2013-03-27 06:42:28 CET
  - Último acceso: 2013-06-19 04:11:24 CEST
- **Hash MD5:** 66a8a952396995a7800ac63e8e2234bd

- **Hash SHA-256:**  
7352059b3e7a29143d0c38dcb8610cbc79251049d41cc8a5866  
2a8101dd2cdf3
- **Tipo:** image/jpeg

image

---

#### 5. kasius 2.jpg - **Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/kasius 2.jpg - **Tamaño:** 5.716 bytes - **MAC Times:** - **Creación:** 2013-06-19 04:11:24 CEST - **Modificación:** 2013-03-27 06:42:04 CET - **Último acceso:** 2013-06-19 04:11:24 CEST - **Hash MD5:** 28f5966b1a4a72cb3b434f688bf8dd0b - **Hash SHA-256:** 1ed78fad0270ba13b15f1222d973cab3f2de072f5d72902af7bc48bd1ac35d - **Tipo:** image/jpeg

---

#### 6. kasius.jpg - **Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/kasius.jpg - **Tamaño:** 9.175 bytes - **MAC Times:** - **Creación:** 2013-06-19 04:11:24 CEST - **Modificación:** 2013-03-27 06:41:58 CET - **Último acceso:** 2013-06-19 04:11:24 CEST - **Hash MD5:** d56befec0c93acbad7fe9d48f5415a2b - **Hash SHA-256:** 28bb98cf7e09a6d96f8bcb4ee5d683740a4a334790f946354df061f175ba20c0 - **Tipo:** image/jpeg

image

## 7. Almacen terraza 4.jpg

- **Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/Almacen terraza 4.jpg
- **Tamaño:** 7.349 bytes
- **MAC Times:**
  - **Creación:** 2013-06-19 04:11:24 CEST
  - **Modificación:** 2013-03-27 06:40:28 CET
  - **Último acceso:** 2013-06-19 04:11:24 CEST
- **Hash MD5:** c641391cfe11009563aaf6d5ff7caf1b
- **Hash SHA-256:**  
c8ab21e06cdcf9524c68f6ab6e2df645a19ebe86fc253a85c052c  
0d5696910cb
- **Tipo:** image/jpeg

image

---

#### 8. Almacen terraza 3.jpg - **Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/Almacen terraza 3.jpg - **Tamaño:** 6.943 bytes - **MAC Times:** - **Creación:** 2013-06-19 04:11:24 CEST - **Modificación:** 2013-03-27 06:39:42 CET - **Último acceso:** 2013-06-19 04:11:24 CEST - **Hash MD5:** 1e6f15394d075ba43308da22ba92059c - **Hash SHA-256:** 805967a139624368bb0c0dd494a0b4c751a649e022b7a32f957d6f592784a - **Tipo:** image/jpeg

---

#### 9. Almacen mataro 3.jpg - **Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/Almacen mataro 3.jpg - **Tamaño:** 14.399 bytes - **MAC Times:** - **Creación:** 2013-06-19 04:11:24 CEST - **Modificación:** 2013-03-27 06:39:26 CET - **Último acceso:** 2013-06-19 04:11:24 CEST - **Hash MD5:** 07e03d5971f5b5a6433a13565cac407d - **Hash SHA-256:**

---

#### 8. Almacen terraza 3.jpg -

**Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/Almacen terraza 3.jpg - **Tamaño:** 6.943 bytes

**MAC Times:** - **Creación:** 2013-06-19 04:11:24 CEST - **Modificación:**

**2013-03-27 06:39:42 CET** - **Último acceso:** 2013-06-19 04:11:24 CEST - **H**

**MD5:** 1e6f15394d075ba43308da22ba92059c - **Hash SHA-256:**

**805967a139624368bb0c0dd494a0b4c751a649e022b7a32f957d6f592784a**

**- Tipo:** image/jpeg

9e75a74404967693442b99278fcce969ddc4f7046903e3fc449b537960e93394 - **T**

image/jpeg

image

---

## 10. Almacen mataro 2.jpg

- **Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/Almacen mataro 2.jpg

- **Tamaño:** 9.935 bytes

- **MAC Times:**

- **Creación:** 2013-06-19 04:11:24 CEST

- **Modificación:** 2013-03-27 06:39:14 CET

- **Último acceso:** 2013-06-19 04:11:24 CEST

- **Hash MD5:** ba0268ffe1d3a340a595cfd9a8cd6b87

- **Hash SHA-256:**

9dd2e70416e70e5099303f04e5d48ad72d27155cf3e8dd5bc50d

cfb93ebc056d

- **Tipo:** image/jpeg

image

---

#### 11. Almacen mataro.jpg - **Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/Almacen

**mataro.jpg** - **Tamaño:** 6.998 bytes - **MAC Times:** - **Creación:** 2013-06-19

**04:11:24 CEST** - **Modificación:** 2013-03-27 06:39:04 CET - **Último acceso:**

**2013-06-19 04:11:24 CEST** - **Hash MD5:**

**c7c5a5521ed005ddad94cb9a9b254d6b** - **Hash SHA-256:**

**5cec8378687c3255665e4123cb30b6e05b2117a8ee9e65fe9a4b986e0cc0fe**

**- Tipo:** image/jpeg

#### 12. Mercancia terraza.jpg - **Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/Mercancia

**terrace.jpg** - **Tamaño:** 8.968 bytes - **MAC Times:** - **Creación:** 2013-06-19 04:11:

**CEST** - **Modificación:** 2013-03-27 06:38:52 CET - **Último acceso:** 2013-06-19

**04:11:24 CEST** - **Hash MD5:** 957894f16f61655cec7110625c7e344b - **Hash**

**SHA-256:**

**bbc8f083cb8bd891463aa62d477620fe884f653e6725ad833f13b312b9f43490** -

**Tipo:** image/jpeg

image

---

## 13. Maria en negocio Jorge.jpg

- **Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/Maria en negocio Jorge.jpg

- **Tamaño:** 5.083 bytes

- **MAC Times:**

- **Creación:** 2013-06-19 04:11:24 CEST



- Modificación: 2013-03-27 06:38:30 CET
- Último acceso: 2013-06-19 04:11:24 CEST
- **Hash MD5:** 18f5a99105c58f8a71a3405562d2eafa
- **Hash SHA-256:**  
b2412594f86335be25a83db0ee9ecaf576f9182a322fe69581ece  
2ccd4d6911f
- **Tipo:** image/jpeg

image

---

**#### 14. mercancia 2.jpg - Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/mercancia 2.jpg - **Tamaño:** 8.620 bytes - **MAC Times:** - **Creación:** 2013-06-19 04:11:24 CEST - **Modificación:** 2013-03-27 06:21:06 CET - **Último acceso:** 2013-06-19 04:11:24 CEST - **Hash MD5:** 5b5a015f4041bbed1bca11fc7be74fcc - **Hash SHA-256:** 25543a3af9f7a0e72fed485116c24a4a45f9705aba49470b1cd891bf8ec8ea0 - **Tipo:** image/jpeg

---

**#### 15. Almacen terrassa.jpg - Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/Almacen terrassa.jpg - **Tamaño:** 9.637 bytes - **MAC Times:** - **Creación:** 2013-06-19 04:11:24 CEST - **Modificación:** 2013-03-27 06:20:50 CET - **Último acceso:** 2013-06-19 04:11:24 CEST - **Hash MD5:** e9bc32019fe6c4bffb1ec9bef18b85aa - **Hash SHA-256:** bd9a18a33b5cec923b6a19d7ddcfb27c580377211761eb602c209d5fb8dfa9bd - **Tipo:** image/jpeg

---

image

## 16. fiesta Jorge.jpg

- **Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/fiesta Jorge.jpg
- **Tamaño:** 8.905 bytes
- **MAC Times:**
  - Creación: 2013-06-19 04:11:24 CEST
  - Modificación: 2013-03-27 06:20:20 CET
  - Último acceso: 2013-06-19 04:11:24 CEST
- **Hash MD5:** c6661d1558b767f31c1f65242af95118
- **Hash SHA-256:**  
bd87c563633f99998dc3956239afcf2b3ea8d19dd8f65e6f483c1  
bc8ca27166e
- **Tipo:** image/jpeg

image

---

#### 17. mercancia.jpg - **Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/mercancia.jpg - **Tamaño:** 6.917 bytes - **MAC Times:** - **Creación:** 2013-06-19 04:11:24 CEST - **Modificación:** 2013-03-27 06:20:08 CET - **Último acceso:** 2013-06-19 04:11:24 CEST - **Hash MD5:** c1481b245fe4f3b5362cd5e19ffaffba - **Hash SHA-256:** 32700fcb07ed7a1c760911c5aa43a24a06afbb42c119fa54197330dc579785 - **Tipo:** image/jpeg

---

#### 18. coca.jpg - **Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/coca.jpg - **Tamaño:** 5.777 bytes - **MAC Times:** - **Creación:** 2013-06-19 04:11:24 CEST - **Modificación:** 2013-03-27 06:19:58 CET - **Último acceso:** 2013-06-19 04:11:24 CEST - **Hash MD5:** 1ffb5afbe2990760fd1b504386593f95 - **Hash SHA-256:** 061c9e9cef4e2f62ddf8ab1e25e7f665037890119f958d385868d752832148c0 - **Tipo:** image/jpeg

---

## 19. pastillas.jpg

- **Ruta:** /img\_AFI\_W.E01/\$OrphanFiles/pastillas.jpg
- **Tamaño:** 12.942 bytes
- **MAC Times:**
  - **Creación:** 2013-06-19 04:11:24 CEST
  - **Modificación:** 2013-03-27 06:19:22 CET
  - **Último acceso:** 2013-06-19 04:11:24 CEST
- **Hash MD5:** 6fe69a3ad25893e824b7c40e252f96a8
- **Hash SHA-256:** 9d51fd7fabfa93a72fcc7b947cc88d12536834756597b7dcf8b155eaf6f5d7c0
- **Tipo:** image/jpeg

image

---

### Documentos y archivos con presuntas conductas delictivas

---

## coca.pdf

- **Ruta:** /img\_AFI\_W.E01/Documents and Settings/John/Desktop/coca.pdf
- **Contenido:** Documento PDF
- **MAC times:**
  - **Modificación:** 2013-03-27 06:46:30 CET
  - **Cambio:** 2013-04-23 02:58:42 CEST
  - **Acceso:** 2013-04-23 02:58:42 CEST
  - **Creación:** 2013-04-23 02:58:42 CEST
- **Tamaño lógico:** 5,826,655 bytes (~5.56 MB)
- **MD5:** e69f1a346f981d322f4ab8105cc3d337
- **SHA-256:** eb312cb66aa5ba35ebd59d8a99b2d46abc54408abddc396d1b593aa91f1dfffb6

image

---

**### manufacturing amfetas.link - Ruta:** /img\_AFI\_W.E01/Documents and Setting  
John/Desktop/manufacturing amfetas.link - **Contenido:** Link - **MAC times:** -  
**Modificación:** 2013-03-28 05:54:58 CET - **Cambio:** 2013-04-23 02:58:52  
CEST - **Acceso:** 2013-05-01 22:05:26 CEST - **Creación:** 2013-04-23 02:58:52  
CEST - **Tamaño lógico:** 133,681 bytes (~130.5 KB) - **MD5:**  
9c555bd582caa34a371fad2487273833 - **SHA-256:**  
1816a7f1bf4100f02a62e87739769654261034df42206ca639db9102439c52

---

**### manufacturing.link - Ruta:** /img\_AFI\_W.E01/Documents and Settings/John/Deskt  
manufacturing.link - **Contenido:** Link - **MAC times:** - **Modificación:** 2013-04-17  
19:22:42 CEST - **Cambio:** 2013-04-23 02:58:52 CEST - **Acceso:** 2013-04-23 02:58:  
CEST - **Creación:** 2013-04-23 02:58:52 CEST - **Tamaño lógico:** 669,101 bytes  
(~653 KB) - **MD5:** 290dfaa70bbb28f0e7a0b4b36b23bd34 - **SHA-256:**  
0200a4b3c5d903519a95731e4c0d12046f6fb21695c232ef7fa0fd148bb63393

image

## providers.ico

- **Ruta:** /img\_AFI\_W.E01/Documents and Settings/John/Desktop/  
providers.ico
- **Contenido:** Icono (.ico)
- **MAC times:**
  - **Modificación:** 2013-04-17 19:24:42 CEST
  - **Cambio:** 2013-03-28 04:10:50 CET
  - **Cambio:** 2013-05-01 22:03:00 CEST
  - **Creación:** 2013-04-23 02:58:35 CEST
- **Tamaño lógico:** 38,400 bytes (~37.5 KB)
- **MD5:** 4a7c3029c15e632ce560f6cb8654e0a2
- **SHA-256:**  
39062606aa7a137116e57956bd03baa1c5ee7e4dacfdc9671658  
870147a21af0

image

---

**### 20130404\_102702.jpg -**  
**Ruta:** /img\_AFI\_W.E01/Documents and Settings/John/My Documents/mataro store/  
20130404\_102702.jpg - **Contenido:** Fotografía JPEG - **MAC times:** - **Modificació**  
**2013-04-04 19:27:02 CEST - Cambio:** 2013-04-23 02:58:06 CEST - **Acceso:**  
**2013-04-23 02:58:06 CEST - Creación:** 2013-04-23 02:58:06 CEST - **Tamañ**  
**lógico:** 3,529,432 bytes (~3.36 MB) - **MD5:**  
a2fc7b3b4276bcebddc25b1bdfa534c8 - **SHA-256:**  
6468370cd5cc1f2011e70de813154b6dec2b1b94b7145997ec0f26ad9ca97a

---

**### 20130404\_102715.jpg - Ruta:** /img\_AFI\_W.E01/Documents and Settings/John/My  
Documents/mataro store/20130404\_102715.jpg - **Contenido:** Fotografía JPEG - **MAC**  
**times:** - **Modificación:** 2013-04-04 19:27:14 CEST - **Cambio:** 2013-04-23 02:58:06  
CEST - **Acceso:** 2013-04-23 02:58:06 CEST - **Creación:** 2013-04-23 02:58:06 CEST  
**Tamaño lógico:** 3,476,592 bytes (~3.31 MB) - **MD5:**

---

### 20130404\_102702.jpg -

**Ruta:** /img\_AFI\_W.E01/Documents and Settings/John/My Documents/mataro store/  
20130404\_102702.jpg - **Contenido:** Fotografía JPEG - **MAC times:** - **Modificación:**  
2013-04-04 19:27:02 CEST - **Cambio:** 2013-04-23 02:58:06 CEST - **Acceso:**  
2013-04-23 02:58:06 CEST - **Creación:** 2013-04-23 02:58:06 CEST - **Tamaño**  
**lógico:** 3,529,432 bytes (~3.36 MB) - **MD5:**  
**a2fc7b3b4276bcebddc25b1bdfa534c8** - **SHA-256:**  
**6468370cd5cc1f2011e70de813154b6dec2b1b94b7145997ec0f26ad9ca97a**

**b63352ab8362d8c51cde10d3112a836f** - **SHA-256:**  
**5268c5fbec4327de490e9abc4474c476f316d4cb5a04d49995357bf7b7bc81c**  
image

---

## store plane.jpg

- **Ruta:** /img\_AFI\_W.E01/Documents and Settings/John/My Documents/  
mataro store/store plane.jpg
- **Contenido:** Fotografía JPEG
- **MAC times:**
  - **Modificación:** 2013-03-27 06:47:56 CET
  - **Cambio:** 2013-04-23 02:58:06 CEST
  - **Acceso:** 2013-04-23 02:58:06 CEST
  - **Creación:** 2013-04-23 02:58:06 CEST
- **Tamaño lógico:** 16,203 bytes (~15.8 KB)
- **MD5:** 7300f60364f28bc5ea67e96b1e1fed24
- **SHA-256:**  
**af1127b988f92ec20d9763d814bf646c13a989306ad28828db06**  
**10fbe9c1c921**

image

---

### proceso final.jpg - **Ruta:** /img\_AFI\_W.E01/Documents and Settings/John/My  
Documents/My Pictures/proceso final.jpg - **Contenido:** Fotografía JPEG - **MAC**  
**times:** - **Modificación:** 2013-03-27 06:43:40 CET - **Cambio:** 2013-04-23  
02:59:26 CEST - **Acceso:** 2013-05-01 22:04:35 CEST - **Creación:** 2013-04-23  
02:59:26 CEST - **Tamaño lógico:** 9,571 bytes (~9.35 KB) - **MD5:**  
**92111747b573b4672293735519a5497f** - **SHA-256:**  
**5b58659dfb74cc396a5f62b290a16c5c939e4d4c18bf9e047e051e5bd9596e**

---

### Metadatos de archivos fotográficos

---

**Archivo:** 20130404\_102715.jpg

**Usuario asociado:** john

**Ruta:** /img\_AFI\_W.E01/Documents and Settings/John/My Documents/  
mataro store/20130404\_102715.jpg

**Tamaño:** 3.476.592 bytes

**Hash MD5:** b63352ab8362d8c51cde10d3112a836f

**Hash SHA-256:**

5268c5fbec4327de490e9abc4474c476f316d4cb5a04d49995357bf7b7bc81c

**Metadatos EXIF encontrados: - Fecha de captura:** 2013-04-04 10:27:14 CEST

- **Dispositivo:** Samsung GT-I8190
- **Latitud:** 41.53260888888889
- **Longitud:** 2.437280555555557
- **Altitud:** 75 m

image

**Observaciones:**

- La foto fue tomada con un teléfono Samsung, lo que puede ser útil para determinar la fuente del archivo.
- La ubicación aproximada indica un punto en Barcelona (aproximadamente), lo que podría relacionar la imagen con un lugar específico de la investigación.
- La fecha y hora de creación coinciden con la fecha de modificación en la imagen forense, lo que ayuda a corroborar la integridad del archivo.

---

### Hojas de cálculo

---

**Archivo 1: contraseñas.xls**

- **Ruta completa:** /img\_AFI\_W.E01/Documents and Settings/John/My Documents/contraseñas.xls
- **Tamaño lógico:** 24.064 bytes
- **Fecha y hora MAC:**
  - Modificación: 2013-04-23 01:34:22 CEST
  - Cambio: 2013-04-23 02:57:53 CEST
  - Acceso: 2013-04-23 02:57:53 CEST
  - Creación: 2013-04-23 02:57:53 CEST
- **Hashes:**
  - MD5: 0a76cd274e4f4750b69cc57a4aa9a5b0
  - SHA-256: 6b3141cdc7414abefb54958a111d357ef4e4fac4a67dc739eda45e9c40e7a7ac
- **Tipo / extensión:** application/vnd.ms-excel / xls
- **Contenido / observaciones:** Archivo protegido con contraseña, no se ha podido acceder al contenido.

image

---

**Archivo 2: Contactes.xls - Ruta completa:** /img\_AFI\_W.E01/Documents and Settings/John/Desktop/Contactes.xls - **Tamaño lógico:** 14.848 bytes - **Fecha y hora MAC:** - **Modificación:** 2013-03-28 05:07:40 CEST - **Cambio:** 2013-04-23 02:58:27 CEST - **Acceso:** 2013-04-23 02:58:27 CEST - **Creación:** 2013-04-23 02:58:27 CEST - **Hashes:** - MD5: 84f9be74d345e59725a8c793e7370d8f - SHA-256: 3bcb717c2dce638850e397de296fa6d37cb59e35312bcc93d7b43c37454fb2 - **Tipo / extensión:** application/vnd.ms-excel / xls - **Contenido / observaciones:** Archivo protegido con contraseña, no se ha podido acceder al contenido.

---

### Ficheros comprimidos

---

#### **Archivo: pedofilia.zip**

- **Usuario asociado:** Ian  
- **Ruta completa:** /img\_AFI\_W.E01/Documents and Settings/Ian/My Documents/My Pictures/pedofilia.zip  
- **Tamaño lógico:** 8.899.826 bytes  
- **Fecha y hora MAC:**  
- Modificación: 2013-03-28 05:33:36 CET  
- Cambio: 2013-04-23 04:08:37 CEST  
- Acceso: 2013-04-23 04:08:37 CEST  
- Creación: 2013-04-23 04:08:36 CEST  
- **Hashes:**  
- MD5: a54529c01bf3a24963ded1fa74579de5  
- SHA-256: 34ce197333d7bd4b5b971039c16adfe36f252880e0c4124bcad4b2f8e119149d  
- **Tipo / extensión:** application/zip / zip  
- **Contenido / observaciones:** Archivo comprimido protegido con encriptación de contenido.

image

---

### Archivos protegidos con contraseña

---

#### **Archivo 1: pedofilia.zip**

- **Ruta completa:** /img\_AFI\_W.E01/Documents and Settings/Ian/My Documents/My Pictures/pedofilia.zip  
- **Tamaño lógico:** 8.899.826 bytes  
- **Tipo / extensión:** application/zip / zip  
- **Protección:** Contenido cifrado con contraseña  
- **Acceso al contenido:** No se pudo acceder al contenido  
- **Observaciones:** El archivo está cifrado, lo que impide acceder a los ficheros internos sin la contraseña correcta. Se han probado ataques de diccionario con rockyou.txt y contraseñas de otros ficheros del sistema sin éxito.

#### **Archivo 2: Contactes.xls**

- **Ruta completa:** /img\_AFI\_W.E01/Documents and Settings/John/Desktop/Contactes.xls  
- **Tamaño lógico:** 14.848 bytes

- **Tipo / extensión:** application/vnd.ms-excel / xls
- **Protección:** Protegido con contraseña
- **Acceso al contenido:** No se pudo acceder al contenido
- **Observaciones:** La hoja de cálculo está protegida, por lo que no se ha podido visualizar ni extraer su contenido.

---

### ### Estudio de la navegación a través de internet

---

En este apartado se presentan los hallazgos relacionados con la navegación por internet de los usuarios del sistema. Se incluyen históricos de navegación, cookies, búsquedas y favoritos/bookmarks. Los hallazgos se asocian, en la medida de lo posible, al usuario correspondiente.

---

#### #### **Historial de navegación (Internet Explorer)**

---

##### **Usuario: Ian**

- [http://www.google.es/search?hl=es&source=hp&q=porn ...](http://www.google.es/search?hl=es&source=hp&q=porn...) (2013-04-23 02:15:39 CEST)
- [http://www.google.es/search?q=porn+pedofil ...](http://www.google.es/search?q=porn+pedofil...) (2013-04-23 02:15:52 CEST)

image

##### **Usuario: John**

- [http://foromotor.foroactivo.com/search?search\\_keywords=drugs](http://foromotor.foroactivo.com/search?search_keywords=drugs) (2013-04-23 02:05:57 CEST)
- [http://www.bluelight.ru/vb/threads/505647-cocaine-in-spain ...](http://www.bluelight.ru/vb/threads/505647-cocaine-in-spain...) (2013-04-24 01:59:42 CEST)

image

---

#### #### **Cookies**

---

##### **Usuario: John**

- john@mataro-parc[1].txt
- Dominio: mataro-parc.com
- Fecha: 2013-05-01 01:01:32 CEST
- Valor: \_\_utma = 89889799.1721614422.1366930823.1366930823.1366930823.1

image

- john@noticias.juridicas[1].txt
  - Dominio: noticias.juridicas.com
  - Fecha: 2013-05-01 01:01:32 CEST
  - Valor: \_\_utma = 262093842.1086171740.1366930865.1366930865.1366930865.1

image

---

### #### **Búsquedas realizadas**

---

#### **Usuario: Ian**

- google.es - porn baby (2013-04-23 02:15:48 CEST)
- google.es - foros pedofilia (2013-04-24 01:58:31 CEST)

image

#### **Usuario: John**

- google.es - building drugs (2013-04-30 23:01:30 CEST)
- google.es - price cocaine spain catalonia (2013-04-30 23:01:30 CEST)
- bing.com - pena delito trafico de droga (2013-04-30 23:01:30 CEST)

image

---

### #### **Favoritos / Bookmarks**

---

#### **Usuario: John**

- Controlled drugs licences, fees and returns - Detailed guidance - GOV.UK
- URL: <https://www.gov.uk/controlled-drugs-licences-fees-and-returns>
- Fecha: 2013-04-23 04:01:09 CEST

image

- CADCA - Building drug-free communities
  - URL: <http://www.cadca.org/>
  - Fecha: 2013-04-23 04:01:29 CEST

image

---

### **Observaciones generales:**

Los historiales, búsquedas y bookmarks muestran un patrón de investigación y posible interés en drogas y pornografía infantil. La información se encuentra asociada principalmente a los usuarios Ian y John, según los registros de Internet Explorer y las cookies extraídas.

---

### ### Otras evidencias relacionadas con conductas delictivas

---

Tras revisar el resto de la imagen forense, no se han encontrado más evidencias relacionadas con otros tipos de conductas delictivas distintas a las ya comentadas en los apartados anteriores.

Se ha comprobado el contenido de los distintos usuarios del sistema, revisando carpetas personales, documentos, imágenes, archivos comprimidos, hojas de cálculo y otros ficheros que



pudieran contener información relevante. También se ha revisado el historial de navegación, búsquedas en internet, cookies y favoritos, así como posibles archivos ejecutables o herramientas sospechosas.

Después de este análisis, no se han localizado indicios de otros delitos como fraudes, estafas, robos de identidad, amenazas, acoso, uso de malware u otro tipo de actividades ilícitas diferentes a las ya descritas.

---

## **6. *Conclusión***

Tras analizar la imagen forense AFI\_WE01, se han encontrado varias evidencias importantes. Destacan documentos, imágenes y búsquedas en internet relacionadas con drogas y otros contenidos ilícitos. También aparecen archivos protegidos con contraseña a los que no se ha podido acceder.

Además, algunos archivos fotográficos contienen metadatos útiles, como la fecha, el dispositivo usado y la localización. En general, la información encontrada es coherente y aporta indicios claros para el análisis del caso.