


Ciberseguridad en  
dispositivos móviles

# Práctica 7

---

Luis López Cuerva  
Pablo Alcarria Lozano



<b>Introducción</b>	<b>2</b>
<b>Recuperación de la imagen</b>	<b>2</b>
<b>Uso de Autopsy para generar un nuevo caso</b>	<b>3</b>
<b>Ejercicio 1 y 2: recuperación de un archivo borrado y su contenido.</b>	<b>4</b>
<b>Ejercicio 3</b>	<b>6</b>
<b>Ejercicio 4</b>	<b>7</b>
<b>Ejercicio 5</b>	<b>7</b>

## Introducción

Durante esta práctica se va a realizar un análisis forense de una imagen extraída de un móvil de un sospechoso de venta de drogas. Durante la práctica se explicarán los programas utilizados para la investigación y los pasos seguidos para conseguir la información de la imagen.

## Recuperación de la imagen

Una vez conseguida la imagen, se hace una copia de ella y se trabaja sobre esa, que se ha renombrado para que tenga el mismo nombre, pero en un directorio distinto. Para comprobar su integridad y que no ha sido modificada se procede a comprobar que la MD5 coincide con la indicada:

“La MD5 de la imagen.zip es b676147f63923e1f428131d59b1d6a72”, vemos que coincide.

“Image”, el contenido dentro del archivo comprimido también coincide con la proporcionada.

```
(kali㉿kali)-[~/Downloads]
$ md5sum image.zip
b676147f63923e1f428131d59b1d6a72  image.zip

(kali㉿kali)-[~/Downloads]
$ md5sum image
ac3f7b85816165957cd4867e62cf452b  image
```

A continuación, generamos un nuevo caso para comenzar la práctica forense.

## Uso de Autopsy para generar un nuevo caso

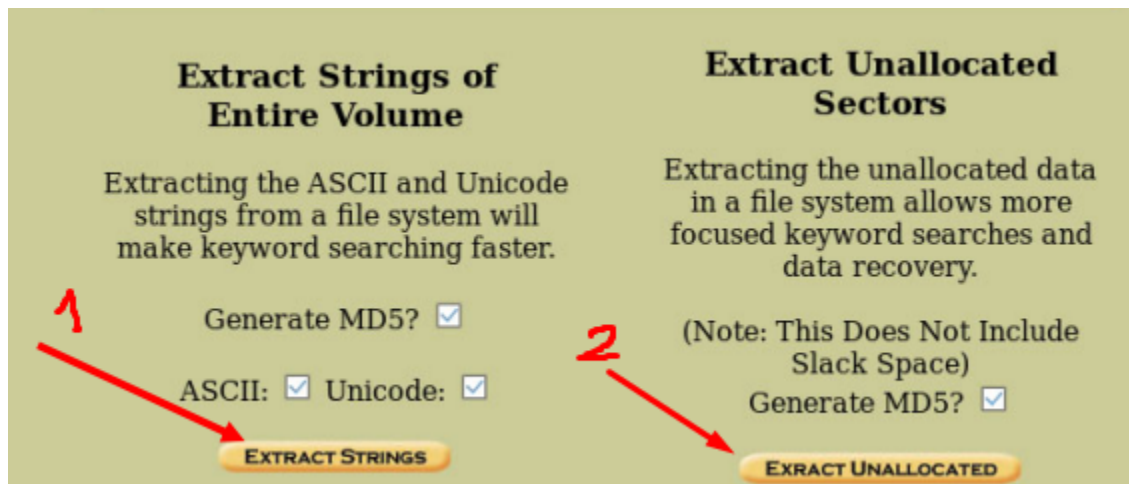
Desde una terminal ejecutamos con privilegios el programa autopsy (sudo autopsy), que nos ejecutará en el puerto local 9999 el programa, y accedemos a él mediante el navegador.

Los pasos para generar el caso son muy sencillos:

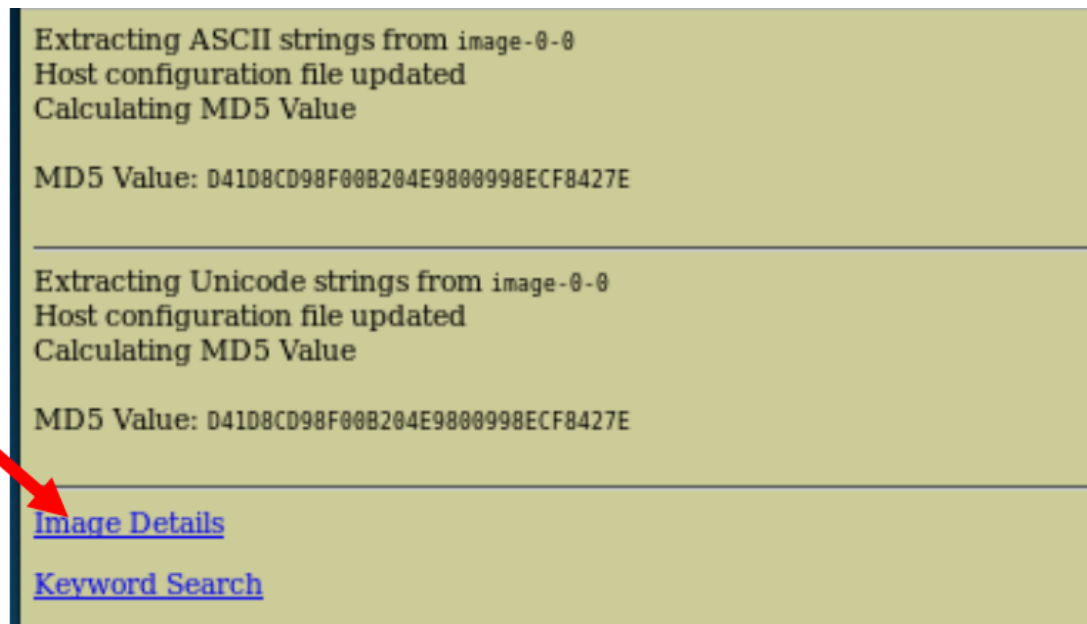
1. Hacer click en “New Case”
2. Rellenamos los datos del formulario: el nombre del caso, una breve descripción, nombres de los investigadores del caso.
3. Creamos el nuevo caso, el programa nos indicará los directorios creados en la máquina para el caso.
4. Añadimos host con el botón “Add Host” que se encuentra al final del formulario.
5. Rellenamos nuevamente el formulario para añadir el host con su nombre, una descripción y la zona horaria. Para finalizar hacemos click en “Add Host”
6. Al agregar el nuevo host, la siguiente pantalla nos solicita añadir una imagen, que es la imagen que hemos comprobado previamente con MD5.
7. Para la inserción de la imagen especificamos su ruta, seleccionando “Disk” en la opción “Type” y “Symlink” en la opción Import Method, para crear un enlace simbólico.
8. Hacemos click en “Next” y entre las dos opciones disponibles escogemos “Volume Image”, dándole a “Ok” para continuar
9. En los detalles del archivo de la imagen escogemos calcular el hash y verificamos antes de importar. Como punto de montaje dejamos “C:” y de sistema de archivos “Fat12”.
10. Finalizamos el proceso haciendo click en el botón “Add”, y en la siguiente ventana “Ok”.

## Ejercicio 1 y 2: recuperación de un archivo borrado y su contenido.

Una vez configurado el caso, tenemos la imagen cargada preparada para analizar. Si hemos montado la imagen como en los pasos señalados, veremos que tenemos montado “C:/” con un sistema de ficheros fat12. Si hacemos click en la opción “details” el programa nos llevará a un apartado en el que podemos extraer los strings del volumen y los sectores sin asignar.



Trabajaremos con la imagen haciendo click en el botón “Extract Strings” y a continuación volveremos a los detalles de la imagen con “Image Details”. Repetimos el proceso con los sectores sin asignar



Después de extraer los datos procedemos al análisis haciendo click en “Analyze” > “File Analysis”.

<div>FILE ANALYSIS   KEYWORD SEARCH   FILE TYPE   IMAGE DETAILS   META DATA   DATA UNIT   HELP   CLOSE</div> <div>🔍</div>										
Current Directory: <a href="#">C:/</a>										
<div>ADD NOTE   GENERATE MD5 LIST OF FILES</div>										
Directory Seek	DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	Error Parsing File (Invalid Characters?): V/V 45782: \$OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0									
		v / v	\$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	45780
		v / v	\$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	45781
		v / v	\$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	45779
File Name Search		r / r	cover_page.jpg	2002-09-11 08:30:52 (GMT)	2002-09-11 00:00:00 (GMT)	2002-09-11 08:50:27 (GMT)	15585	0	0	8
	✓	r / r	JimmyJungle.doc	2002-04-15 14:42:30 (GMT)	2002-09-11 00:00:00 (GMT)	2002-09-11 08:49:49 (GMT)	20480	0	0	5
		r / r	ScheduledVisits.exe	2002-05-24 08:20:32 (GMT)	2002-09-11 00:00:00 (GMT)	2002-09-11 08:50:38 (GMT)	1000	0	0	11
<div>SEARCH</div> <div>ALL DELETED FILES</div> <div>EXPAND DIRECTORIES</div>										
<div>ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note</div> <div>File Type: ERROR-[gzip: Exec 'gzip' failed, No such file or directory] (Zip archive data, at least v2.0 to extract)</div> <div>00000268: 08C2 1818 9581 0010 4202 4735 81F8 0948 .....B.G5...K 00000270: 5F1D 94C0 1825 240C 7907 E288 2083 0385 ....N.y..... 00000300: 3806 465A 8C7D 22C4 8632 9095 0676 7790 0H2.J'.2...w. 00000310: 5DC0 1331 432F 2B4E E786 878E 141C C9F9 }.1C/N.f..... 00000320: 82CA 6121 FAB0 A3DA 096A DAEC C687 9E12 ..al..... 00000330: 0256 439E 809F 10F0 7607 0476 790C D1F9 ..VC....v.vy.. 00000340: 99C1 0596 F854 1425 2941 9058 2523 24EA ....T.A.XW\$. 00000350: CD67 5E89 0ECD 4F8B 34E3 F455 191F 0808 ...0.4..U... 00000360: 9E96 70D7 3C44 17FC 5421 9083 787A A011 ...}..0..T..x2..</div>										

Entre los archivos nos encontramos “cover page.jpg”, “JimmyJungle.doc” y “ScheduledVisits.exe”. “JimmyJungle.doc” está con un color rojo ya que se reconoce como un archivo eliminado por Autopsy. Para analizarlo, hacemos click en el valor de “Meta”, es decir, el 5.

Se calcula el número de sectores del archivo para recuperarlo: Desde el sector 32 al 72, son 40 sectores. Con la información conseguida, indicamos el número del sector principal (33) y el calculado (40), haciendo click en “view” para ver el contenido. En hexadecimal nos encontramos con que los magic numbers nos dicen la extensión del archivo, pero si mostramos el contenido

en ASCII podemos ver suficiente texto como para conseguir la dirección y el nombre de su proveedor: Jimmy, que vive en 626 Jungle Ave Apt 2, en NY 11111.

The screenshot shows a forensic tool interface with a left sidebar and a main content area. The sidebar contains fields for 'Sector Number' (33), 'Number of Sectors' (40), 'Sector Size' (512), 'Address Type' (Regular (dd)), and 'Lazarus Addr'. Below these are buttons for 'VIEW', 'ALLOCATION LIST', and 'LOAD UNALLOCATED'. The main content area has a top bar with navigation buttons (PREVIOUS, NEXT, EXPORT CONTENTS, ADD NOTE) and a status bar showing 'ASCII (display - report) \* Hex (display - report) \* ASCII Str' and 'File Type: Composite Document File V2 Document'. The main area displays 'Sectors: 33-72' and 'Status: Not Allocated' with a link to 'Find Meta Data Address'. Below this is a large ASCII dump. A red box highlights the text '626 Jungle Ave Apt 2' and 'Jungle, NY 11111'. Below the highlighted text is a block of text starting with 'Jimmy:' and a letter from Joe.

Sector Number: 33  
Number of Sectors: 40  
Sector Size: 512  
Address Type: Regular (dd)  
Lazarus Addr: ☐  
VIEW  
ALLOCATION LIST  
LOAD UNALLOCATED

PREVIOUS NEXT  
EXPORT CONTENTS ADD NOTE  
ASCII (display - report) \* Hex (display - report) \* ASCII Str  
File Type: Composite Document File V2 Document

Sectors: 33-72  
Status: Not Allocated  
Find Meta Data Address

626 Jungle Ave Apt 2  
Jungle, NY 11111

Jimmy:

Dude, your pot must be the best . it made the cover of High Times Magazine! Thanks for sending me the Cover Page. What do you  
it and not some guy in Columbia.

These kids, they tell me marijuana isn.t addictive, but they don.t stop buying from me. Man, I.m sure glad you told me about t  
guaranteed paycheck. Their parents give them money for lunch and they spend it on my stuff. I.m an entrepreneur. Am I only one

I emailed you the schedule that I am using. I think it helps me cover myself and not be predictive. Tell me what you think. T  
you later.

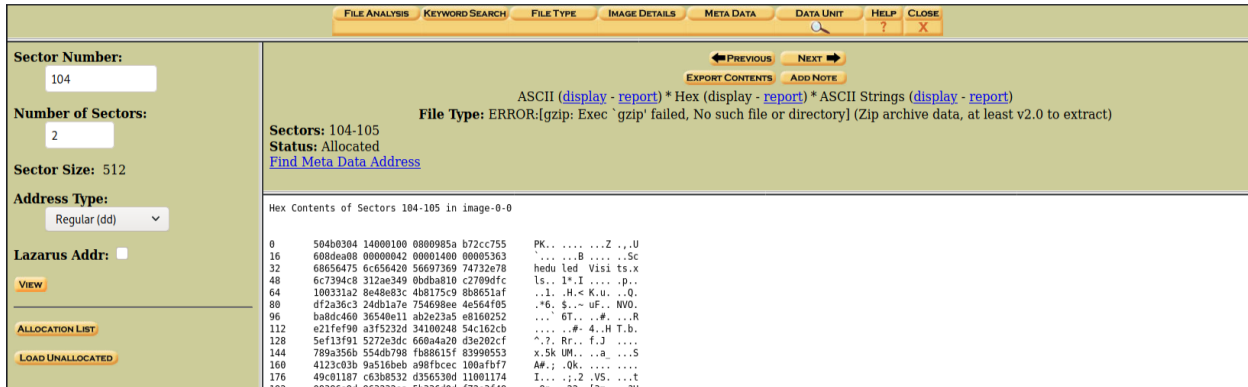
Thanks,

Joe

Este contenido debemos exportarlo con “Export contents”, que nos lo dejará descargar con una extensión “.raw” indicando que es un archivo “en crudo”, por lo que es necesario cambiar la extensión del archivo para poder visualizarlo correctamente con el programa adecuado.

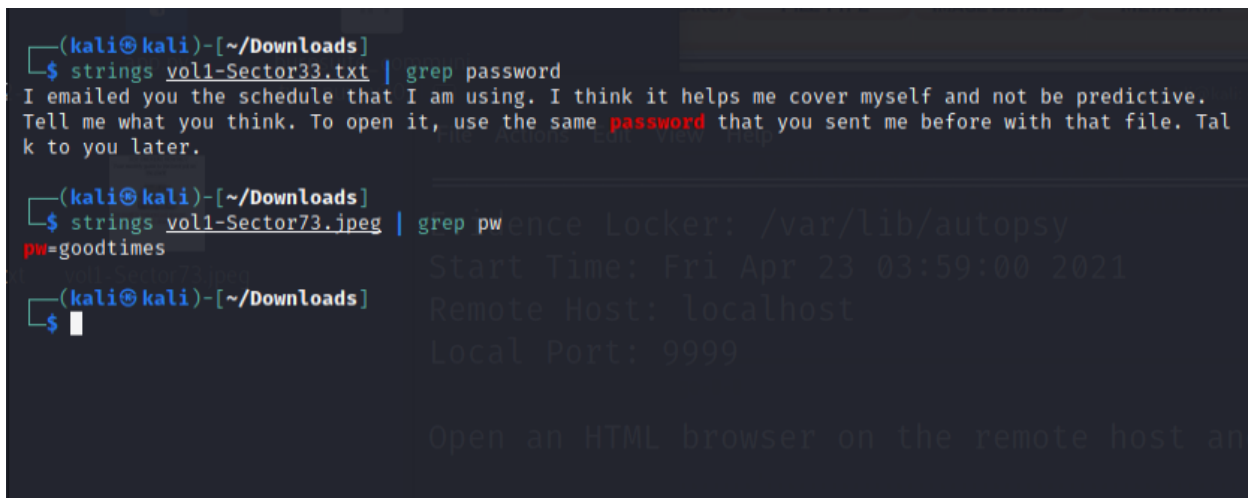
## Ejercicio 3

El fichero Secheduled Visits.exe consta de dos volúmenes, el 104 y 105. Además en el magic number del fichero se puede ver que el formato es .zip



## Ejercicio 4

La contraseña del fichero zip es goodtimes, para encontrarla hemos buscado en el fichero JimmyJungle.doc la palabra password y hemos leído que la contraseña se la dijo en el cartel, de manera que hemos buscado un string en el cartel y la hemos encontrado.



## Ejercicio 5

En el fichero ScheduledVisits se puede encontrar que Joe Jacobs frecuenta los institutos que se observan en la imagen.



```
kali@kali: ~/Downloads/New Folder
File Actions Edit View Help
$ strings Scheduled\ Visits.xls
CSTC
"$",##0_);\("$",##0\
"$",##0_);[Red]\("$",##0\
"$",##0.00_);\("$",##0.00\
"$",##0.00_);[Red]\("$",##0.00\
_("$" * #,##0_);\("$" * \(#,##0\);\("$" * "-";_(@_
_(* #,##0_);\(* \(#,##0\);\(* "-";_(@_
_("$" * #,##0.00_);\("$" * \(#,##0.00\);\("$" * "-";_(@_
_(* #,##0.00_);\(* \(#,##0.00\);\(* "-";_(@_
Sheet1
Sheet2
Sheet3
HIGH SCHOOLS
Monday (1)
Tuesday (2)
Wednesday (3)
Thursday (4)
Friday (5)
Smith Hill High School (A)
Key High School (B)
Leetch High School (C)
Birard High School (D)
Richter High School (E)
Hull High School (F)
Month
April and paste this URL in it:
June
MbP?_
DINU"
```