



# UNIVERSIDAD LUTERANA SALVADOREÑA

FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA  
LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

## NOMBRE DEL PROYECTO

**MATERIA**

**ANÁLISIS DE SISTEMAS**

CICLO II-2017

### INTEGRANTES:

| Carnet     | Apellidos        | Nombres         |
|------------|------------------|-----------------|
| Gh02110140 | García Hernández | Pedro Antonio   |
| BL01132837 | Bermúdez Luna    | Alisson Dinora  |
| SP01132149 | Saravia Penado   | Sonia Elizabeth |

### DOCENTE:

LIC. JOSÉ LUIS ALVARADO AGUILAR

SAN SALVADOR 11 DE NOVIEMBRE DE 2017

## PRESENTACIÓN

Los archivos que almacenamos, creamos, y gestionamos a diario desde nuestros dispositivos esconden en su interior datos que la mayoría de los usuarios desconocen; hoy aprenderemos a localizarlos, editarlos, o eliminarlos con la herramienta ExifTool.

Estos se llaman metadatos, y sirven para gestionar los archivos dentro del sistema entre otras cosas, un ejemplo podría ser la hora y el minuto de la última edición, el modelo de la cámara que tomó una fotografía, la ubicación geográfica desde donde fue tomada la imagen mediante las coordenadas GPS, o conocer que software ha empleado el usuario para su creación o edición.

Se ha dado mas de un caso en el que los metadatos han jugado malas pasadas, por ejemplo el caso del Defacer que colgó una foto del escote de su novia en la portada de la web que hackeó, sin eliminar las coordenadas GPS de la imagen que había tomado con su “flamante” Iphone.

## **JUSTIFICACIÓN**

En primer lugar debemos saber que los metadatos no son más que información que se agrega a los contenedores multimedia para poder clasificarlos de una forma eficiente. Los archivos de video con extensión .mp4, .mkv, .mov, .wmv, etc... pueden contener metadatos.

Hemos elegido ExifTool porque es quizás la herramienta más completa y más potente para gestionar los metadatos de archivos multimedia. Además es una herramienta gratuita que soporta muchísimos formatos de contenedores multimedia (por no decir la práctica totalidad).

Los metadatos están cada vez más presentes y en ocasiones pueden suponer un riesgo para nuestra privacidad. El mejor de los ejemplos sucede cuando empleamos un smartphone para tomar una foto, ya que este puede añadir metadatos con las coordenadas GPS de donde se realizó la foto, algo que puede suponer un problema a la hora de compartirla en las redes sociales.

## **OBJETIVO GENERAL**

**Conocer** lo que son los metadatos para que sirven como funcionan y demás.

## **OBJETIVOS ESPECÍFICOS**

**Dar** a conocer una herramienta que pocos conocen y que es de gran ayuda si se sabe usar.

**Proporcionar** datos y usos de la herramienta Exiftool.

## ANTECEDENTES

Exiftool una herramienta desarrollada en Perl la cual la tenemos tanto para Windows, Linux, Mac y que habitualmente es a base de comandos desde la terminal. Exiftool nos permite extraer la metadato de una imagen en este caso saque una foto la cual tenia activado, el GPS.

A pesar de que podría decirse que esta aplicación de nombre Exiftool viene a ser el método sencillo, dependiendo del conocimiento de informática y de manejo de comandos, para alguien podría ser una de las tareas más difíciles para ejecutar. Exiftool es una aplicación gratuita de apenas 3.6 mega bytes, misma que esta disponible tanto para Windows, Linux o Mac, y cuyas versiones las podrás descargar desde su enlace oficial.

Exiftool es un programa de software con el que podemos acceder y manipular los metadatos de una gran variedad de formatos (JPEG, PNG, MP3, PDF, WEBM, RAR, RTF, SWF, PDF, RAW, PSD o PSP...) incluyendo archivos de video, sonido, imágenes o texto.

## **MATERIALES Y MÉTODOS**

### **1. Área de estudio:**

Universidad Luterana Salvadoreña

### **2. Materiales y equipos:**

2 Computadoras con sistema debían

Archivos para eliminar metadatos

Internet

### **Métodos y procedimientos:**

#### **3.**

Como grupo se ha tomado a bien realizar el proceso siguiente:

Nos informaremos al máximo sobre a herramienta a utilizar .

Se realizaran pruebas previas

Se corregirán errores

Realizaremos pruebas de ser posible finales.

Se hará un manual escrito

Se entregará

#### **4. Duración:**

Inicio: 06 de Noviembre de 2017

Finalización: 01 de diciembre de 2017

## PRESUPUESTO

| <b>Detalle</b>         | <b>Costo</b> |
|------------------------|--------------|
| Internet               | \$30 .00     |
| Depreciación de equipo | \$100.00     |
| Impresiones            | \$30.00      |
| Imprevistos            | \$40.00      |
| Total                  | \$200.00     |

## CRONOGRAMA DE ACTIVIDADES

| Fecha  | 06-11<br>Nov.   | 12-17<br>Nov                  | 19-25<br>Nov                                 | 26-1 Dic                |
|--|---|-------------------------------|--|-------------------------|
| Actividad                                    |   |                               |  |                         |
| <b>E<br/>X<br/>I<br/>F<br/>T<br/>O<br/>I</b> | Nos informaremos al máximo sobre a herramienta a utilizar | .                             |  |                         |
|  | Se instalará herramienta                                  | Se realizaran pruebas previas | Se hará un manual escrito                    |                         |
|  |   | Se corregirán errores         | Realizaremos pruebas de ser posible finales. |                         |
|  |   |                               |  | Entrega documento final |



## ANEXOS

### 1.0 datos de un archivo png.

```
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
root@PedroPc:/home/pedro# exiftool -a '/home/pedro/Descargas/Screenshot_2017-05-21-22-44-53.png'
ExifTool Version Number      : 10.40
File Name                    : Screenshot_2017-05-21-22-44-53.png
Directory                   : /home/pedro/Descargas
File Size                    : 342 kB
File Modification Date/Time  : 2017:10:09 10:12:11-06:00
File Access Date/Time       : 2017:11:10 15:25:31-06:00
File Inode Change Date/Time  : 2017:10:09 10:12:11-06:00
File Permissions             : rw-----
File Type                    : PNG
File Type Extension         : png
MIME Type                    : image/png
Image Width                  : 480
Image Height                 : 800
Bit Depth                    : 8
Color Type                   : RGB
Compression                  : Deflate/Inflate
Filter                       : Adaptive
Interlace                    : Noninterlaced
Significant Bits             : 8 8 8
Image Size                   : 480x800
Megapixels                   : 0.384
root@PedroPc:/home/pedro#
```

### 1.1 Metadatos de un archivo de pdf.

```
root@PedroPc:/home/pedro# exiftool -a '/home/pedro/Escritorio/pensumcomputacion2014.pdf'
ExifTool Version Number      : 10.40
File Name                    : pensumcomputacion2014.pdf
Directory                   : /home/pedro/Escritorio
File Size                    : 583 kB
File Modification Date/Time  : 2017:11:07 22:09:52-06:00
File Access Date/Time       : 2017:11:07 22:09:59-06:00
File Inode Change Date/Time  : 2017:11:07 22:09:59-06:00
File Permissions             : rw-r--r--
File Type                    : PDF
File Type Extension         : pdf
MIME Type                    : application/pdf
PDF Version                  : 1.4
Linearized                   : No
Page Count                   : 1
Language                     : es-ES
Creator                      : Writer
Producer                     : LibreOffice 4.2
Create Date                  : 2015:05:27 09:27:10-06:00
root@PedroPc:/home/pedro#
```

## 1.2 metadatos de un archivo img.

```
root@PedroPc:/home/pedro# exiftool '/home/pedro/Descargas/IMG-20171003-WA0000.jpg'
ExifTool Version Number      : 10.40
File Name                    : IMG-20171003-WA0000.jpg
Directory                   : /home/pedro/Descargas
File Size                    : 20 kB
File Modification Date/Time  : 2017:10:09 10:15:03-06:00
File Access Date/Time       : 2017:11:08 19:53:13-06:00
File Inode Change Date/Time  : 2017:10:09 10:15:03-06:00
File Permissions             : rw-----
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
JFIF Version                : 1.01
Resolution Unit             : None
X Resolution                 : 72
Y Resolution                 : 72
Image Width                  : 480
Image Height                 : 801
Encoding Process            : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components             : 3
Y Cb Cr Sub Sampling        : YCbCr4:2:0 (2 2)
Image Size                   : 480x801
Megapixels                   : 0.384
root@PedroPc:/home/pedro#
```

## 1.3 metadatos de un archivo odt.

```
root@PedroPc:/home/pedro# exiftool '/home/pedro/Descargas/informática Jurídica.odp'
ExifTool Version Number      : 10.40
File Name                    : informática Jurídica.odp
Directory                   : /home/pedro/Descargas
File Size                    : 21 kB
File Modification Date/Time  : 2017:11:01 19:00:58-06:00
File Access Date/Time       : 2017:11:10 20:35:56-06:00
File Inode Change Date/Time  : 2017:11:01 19:00:58-06:00
File Permissions             : rw-r--r--
File Type                   : ODP
File Type Extension         : odp
MIME Type                   : application/vnd.oasis.opendocument.presentation
Title                       : INFORMATICA JURIDICA
Initial-creator              : Karla Mendoza
Editing-cycles               : 4
Creation-date                : 2017:10:30 16:47:06
Date                        : 2017:10:30 19:41:52.599000000
Editing-duration             : PT35M55
Generator                    : LibreOffice/5.4.0.3$Windows_x86 LibreOffice_project/7556cbc6811c9d992f4064ab9287069087d7f62c
Document-statistic Object-count : 69
User-defined Name           : AppVersion
User-defined                 : 15.0000
User-defined Value-type     : float
Template Type                : simple
Template Actuate             : onRequest
Template Title               : Distintivo
Template Href                :
Preview PNG                  : (Binary data 4151 bytes, use -b option to extract)
root@PedroPc:/home/pedro#
```

Enlaces de videos.

<https://youtu.be/KuvLcpbwzF0>

## **BIBLIOGRAFÍA**

<http://www.javiertobal.com/herramientas-linux-para-analisis-forense-detalle/>

<https://www.welivesecurity.com/la-es/2016/02/23/distribuciones-gratuitas-analisis-forense/>

<https://phyx.wordpress.com/2008/12/12/foremost-recuperacion-de-archivos-borrados-desde-la-linea-de-comandos/>

<https://prezi.com/kcoki3kq5wsj/21-herramientas-mas-populares-de-informatica-forense/>

<http://conexioninversa.blogspot.com/2013/09/forensics-powertools-listado-de.html>