

Anexo 12: Datos de Fotografías y como nos pueden seguir el rastro.

Hoy en día es muy popular ir realizándose con el teléfono móvil multitud de fotografías de las cuales muchas terminan en nuestras redes sociales y correos electrónicos.

Pero existe un peligro, del cual no nos hemos dado cuenta o si nos hemos dado cuenta pensamos que no existe ningún problema.

Cada vez que tomamos una foto, da igual con que tipo de cámara, dejan inscritas dentro de la fotografía unos datos que se llaman EXIF. Es como una huella digital que deja cada fotografía. No se ven a simple vista y entre ellos se encuentra la fecha, hora y lugar en el que se hicieron las fotos.

Si somos personas confiables en que todo esta bien y que esto no tiene que ver con seguridad, pueden parar y dejar de seguir el curso.

Para las personas que piensan que su seguridad puede estar en peligro, sigamos adelante.

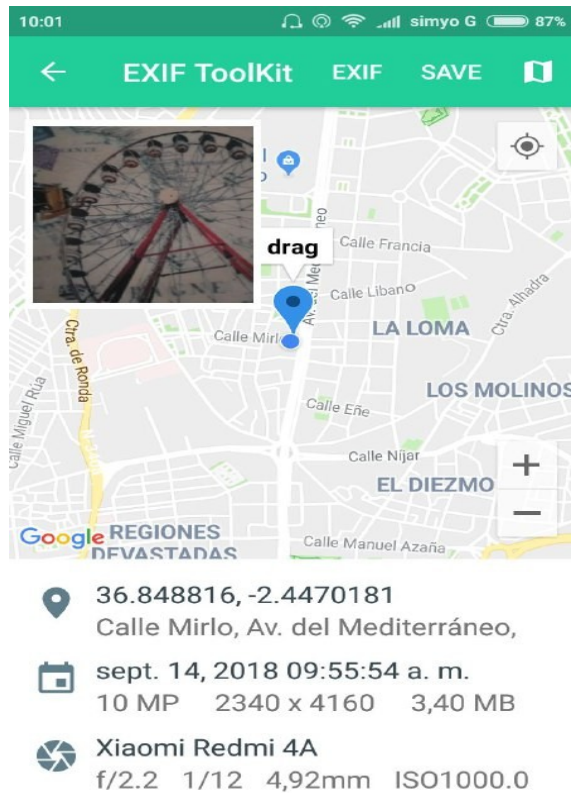
Inocentemente acabamos de sacar una fotografía de un Poster de una habitación de un hotel y queremos que todos nuestros amigos puedan verlas y las colocamos en todas las redes sociales...



Anexo 12. Formador Fabio Quintero Pérez

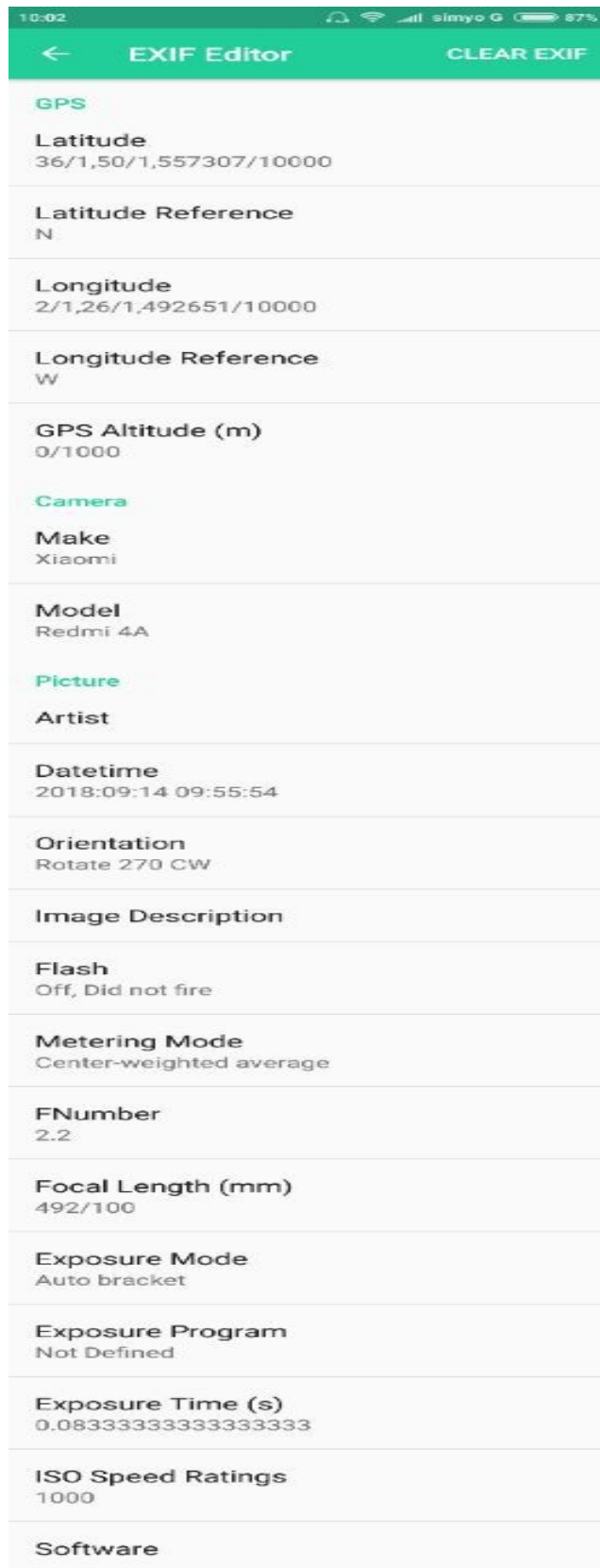
La fotografía es muy bonita, pero aunque creemos que sólo mandamos una foto, mandamos un montón de datos que una persona cualquiera no sepa o pueda ver, pero en las que un hacker si.

Si el hacker mira la información básica podrá ver esto:



FECHA, HORA E INCLUSO LA DIRECCIÓN EN DÓNDE SE HIZO LA FOTO.

Si quisiera ver una información mucho más pormenorizada y con más detalles, vería esto:



The screenshot shows a mobile application interface titled "EXIF Editor". At the top, there is a green header bar with a back arrow on the left, the text "EXIF Editor" in the center, and "CLEAR EXIF" on the right. Below the header, the interface is divided into several sections, each with a green title and a list of metadata items. The sections are: GPS, Camera, Picture, and Software. Each section contains a bold title followed by its value.

Section	Field	Value
GPS	Latitude	36/1,50/1,557307/10000
	Latitude Reference	N
	Longitude	2/1,26/1,492651/10000
	Longitude Reference	W
	GPS Altitude (m)	0/1000
Camera	Make	Xiaomi
	Model	Redmi 4A
Picture	Artist	
	Datetime	2018:09:14 09:55:54
	Orientation	Rotate 270 CW
	Image Description	
	Flash	Off, Did not fire
	Metering Mode	Center-weighted average
	FNumber	2.2
	Focal Length (mm)	492/100
	Exposure Mode	Auto bracket
	Exposure Program	Not Defined
	Exposure Time (s)	0.083333333333333333
	ISO Speed Ratings	1000
Software		

Ahora el hacker puede utilizar esa información, y por ejemplo pasársela a un grupo de ladrones que se encargarían de desvalijarte el piso o pasárselo a un grupo de mafiosos para realizar un rapto y pedir un rescate, ya que durante 2 o 3 días, estás mandando fotos sobre los lugares que visitas, bares, pubs, peluquerías,... O alguien puede tomar venganzas sobre ti...

Por eso es muy importante saber que datos proporcionamos en las redes sociales y a quien. (Tener 2000 amigos o seguidores en redes sociales solo implica un número (una estadística) más en la red (muchos son bots (robots) aleccionados para sacar información.

Para esto existen 2 soluciones:

- Revisar cada foto que quieras publicar y borrar los metadatos (EXIF) que consideres comprometedores.
- Configurar la cámara de tu smartphone, para que no añada datos sensible como la ubicación GPS en las fotografías que haceis.