

## UD1. Adopción de pautas de seguridad informática. Legislación

### Tarea 4 - Esteganografía

#### Parte 1.

Vamos a utilizar un programa para ocultar mensajes en una imagen. Se trata de OpenStego.

- Busca la página web oficial, descarga el fichero `.deb` e instálalo en tu máquina virtual.
- Averigua cómo introducir un mensaje dentro de una imagen y hazlo. Asegúrate de proteger el mensaje con una contraseña.
- Adjunta en Aules la imagen con el mensaje escondido. Asegúrate de recordar la contraseña para que le profesor pueda extraer el mensaje.
- Ahora descarga la imagen **Homer.png** y averigua cuál es el mensaje oculto. La contraseña utilizada es *mipassword*.

#### Parte 2.

A pesar de que no se trata directamente de esteganografía, en Kali Linux encontramos herramientas que nos van a permitir extraer información de las imágenes. Uno de los usos más peligrosos que tienen estas herramientas es el de geolocalizar dichas imágenes. Cuando realizamos fotos con los móviles, es muy probable que tengamos activada la geolocalización de las imágenes, con lo que dicha información se guarda en la propia imagen. Si esas imágenes se suben a Internet, un atacante podría utilizar las herramientas que comentamos para averiguar dónde fue tomada dicha fotografía.

- Echa un vistazo a la herramienta `exiftool`. Descarga la imagen *IMG\_20190421\_174525.jpg* y averigua dónde y en qué fecha fue tomada dicha fotografía.