

# GRAMPUS - GUÍA DE USUARIO



## Índice :

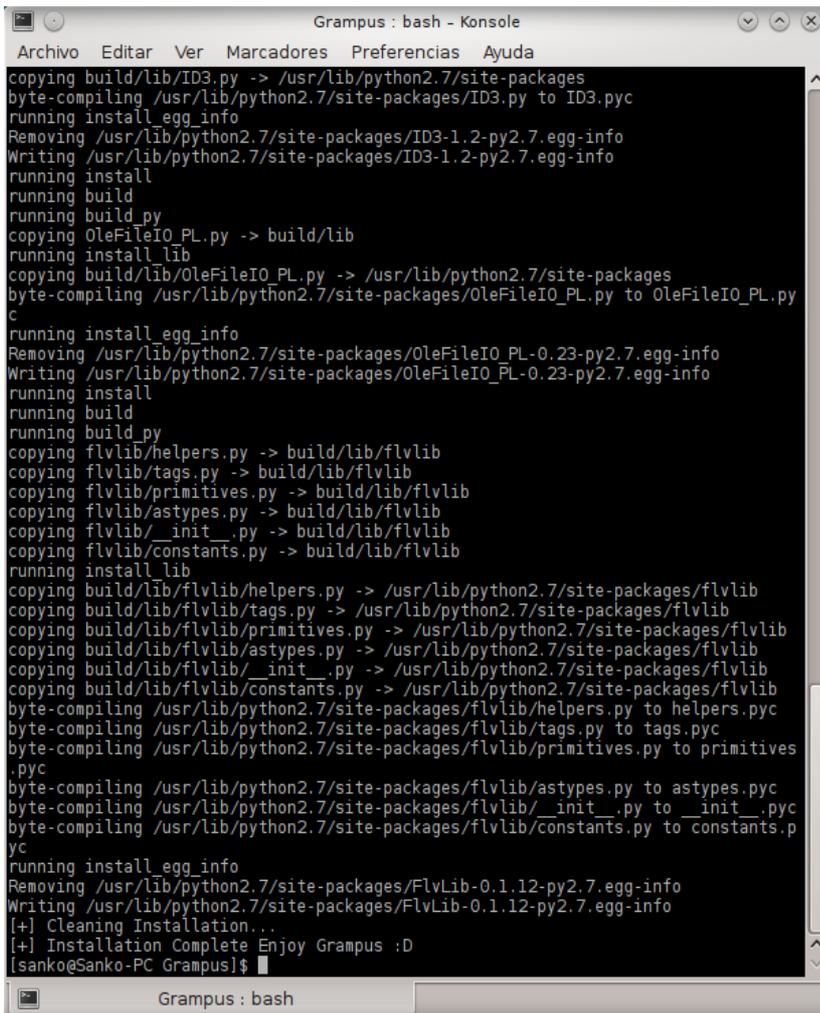
- Instalación
- Ejecución
- Extraer metadatos de archivos
- Limpiar metadatos de archivos
- Uso de los crawlers
- Uso de las tareas de fingerprinting

# Instalación :

Empezemos con la instalación de las dependencias que harán correr la herramienta. Dentro del directorio se encuentra un archivo llamado “setup.py”, abrimos la terminal/cmd y escribimos :

“ *python setup.py install* “

De correrlo desde un terminal GNU/Linux, Unix, debemos darnos permisos para realizar las tareas.



```
Grampus : bash - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
copying build/lib/ID3.py -> /usr/lib/python2.7/site-packages
byte-compiling /usr/lib/python2.7/site-packages/ID3.py to ID3.pyc
running install_egg_info
Removing /usr/lib/python2.7/site-packages/ID3-1.2-py2.7.egg-info
Writing /usr/lib/python2.7/site-packages/ID3-1.2-py2.7.egg-info
running install
running build
running build_py
copying OleFileIO_PL.py -> build/lib
running install_lib
copying build/lib/OleFileIO_PL.py -> /usr/lib/python2.7/site-packages
byte-compiling /usr/lib/python2.7/site-packages/OleFileIO_PL.py to OleFileIO_PL.pyc
running install_egg_info
Removing /usr/lib/python2.7/site-packages/OleFileIO_PL-0.23-py2.7.egg-info
Writing /usr/lib/python2.7/site-packages/OleFileIO_PL-0.23-py2.7.egg-info
running install
running build
running build_py
copying flvlib/helpers.py -> build/lib/flvlib
copying flvlib/tags.py -> build/lib/flvlib
copying flvlib/primitives.py -> build/lib/flvlib
copying flvlib/astypes.py -> build/lib/flvlib
copying flvlib/__init__.py -> build/lib/flvlib
copying flvlib/constants.py -> build/lib/flvlib
running install_lib
copying build/lib/flvlib/helpers.py -> /usr/lib/python2.7/site-packages/flvlib
copying build/lib/flvlib/tags.py -> /usr/lib/python2.7/site-packages/flvlib
copying build/lib/flvlib/primitives.py -> /usr/lib/python2.7/site-packages/flvlib
copying build/lib/flvlib/astypes.py -> /usr/lib/python2.7/site-packages/flvlib
copying build/lib/flvlib/__init__.py -> /usr/lib/python2.7/site-packages/flvlib
copying build/lib/flvlib/constants.py -> /usr/lib/python2.7/site-packages/flvlib
byte-compiling /usr/lib/python2.7/site-packages/flvlib/helpers.py to helpers.pyc
byte-compiling /usr/lib/python2.7/site-packages/flvlib/tags.py to tags.pyc
byte-compiling /usr/lib/python2.7/site-packages/flvlib/primitives.py to primitives.pyc
byte-compiling /usr/lib/python2.7/site-packages/flvlib/astypes.py to astypes.pyc
byte-compiling /usr/lib/python2.7/site-packages/flvlib/__init__.py to __init__.pyc
byte-compiling /usr/lib/python2.7/site-packages/flvlib/constants.py to constants.pyc
running install_egg_info
Removing /usr/lib/python2.7/site-packages/FlvLib-0.1.12-py2.7.egg-info
Writing /usr/lib/python2.7/site-packages/FlvLib-0.1.12-py2.7.egg-info
[+] Cleaning Installation...
[+] Installation Complete Enjoy Grampus :D
[sanko@Sanko-PC Grampus]$
```

Una vez finalizada la instalación, ya podemos proceder a abrir la GUI.

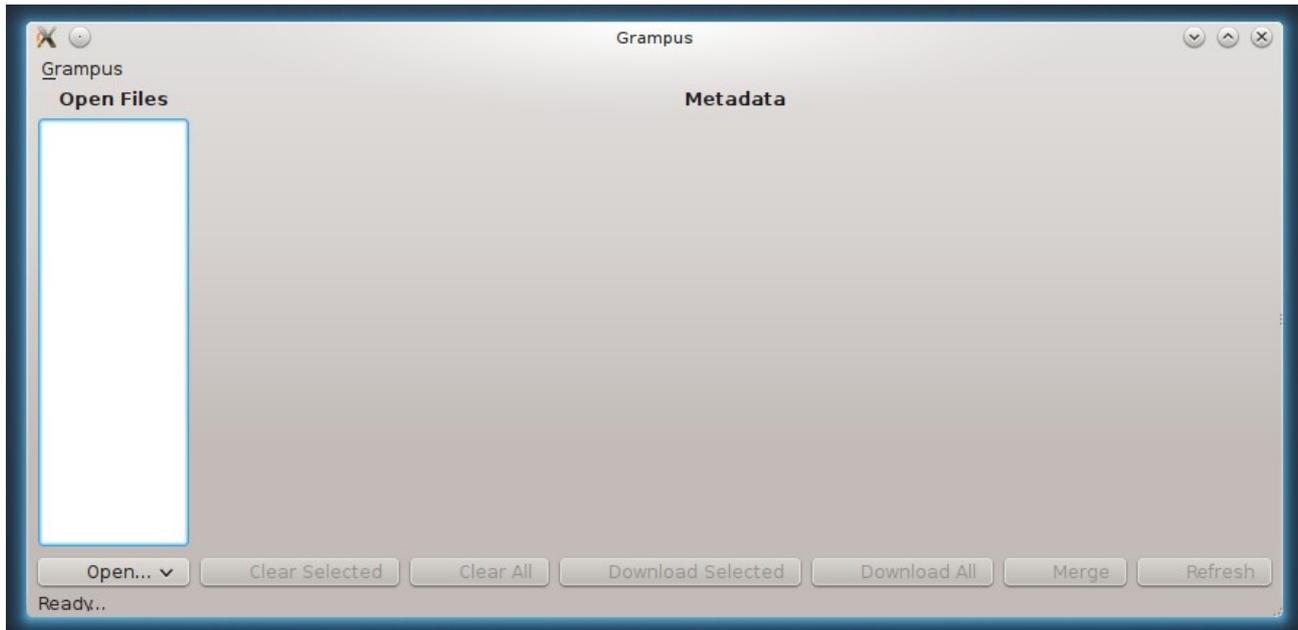
En caso de error durante la instalación se aconseja una instalación manual de las librerías.

## Ejecución :

Una vez ya tenemos las dependencias instaladas podemos pasar a la ejecución de la GUI, escribimos en terminal/cmd :

```
python MainGrampus.py
```

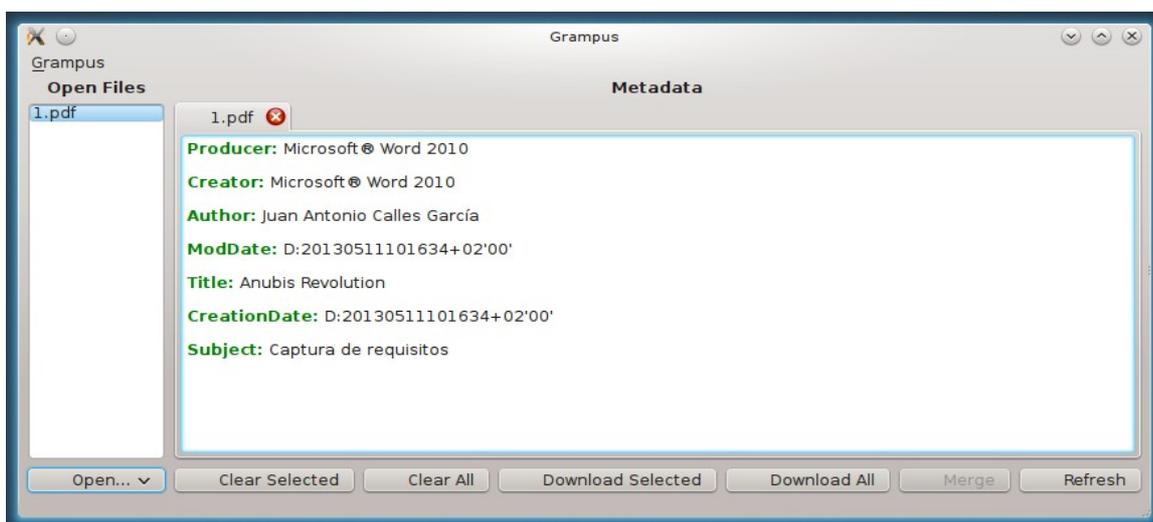
y se nos abrirá la interfaz gráfica :



## Extraer metadatos de archivos :

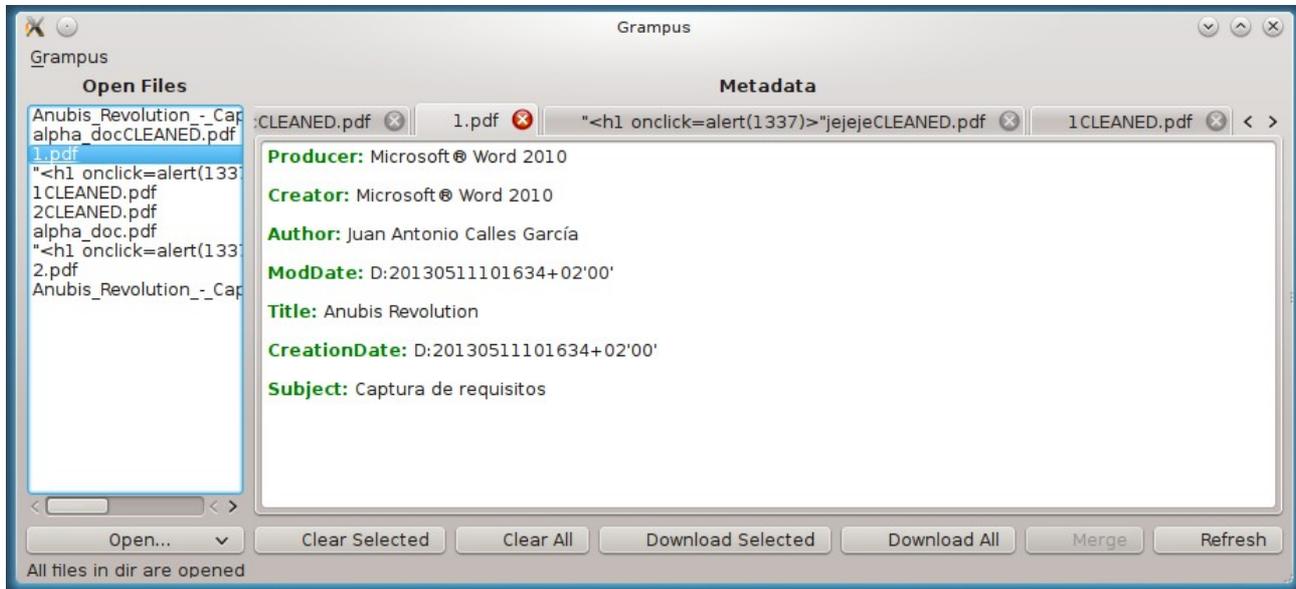
### • Archivos individuales :

Para extraer los metadatos de archivos de manera individual, nos desplazamos hasta el botón “Open” donde nos aparecerá la opción de abrir un archivo “file” y seleccionamos el archivo deseado para su instantanea extracción.



## • Directorios :

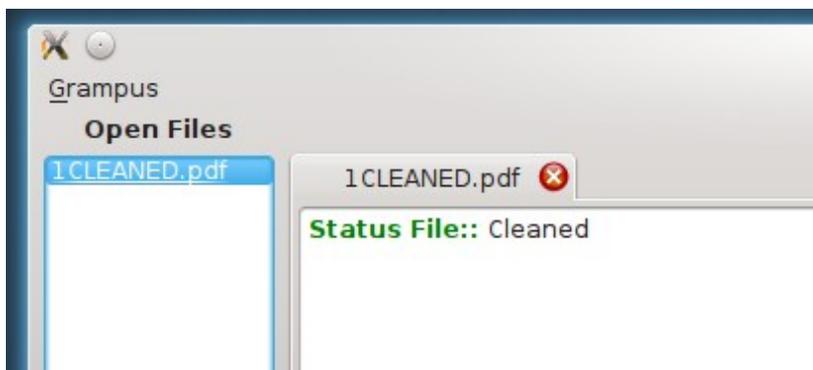
Para extraerlos metadatos de todos los archivos contenidos en un directorio, solo tenemos que desplazarnos hasta el botón “Open” > “Directory”, una vez hecho esto seleccionamos el directorio en el que tenemos contenidos todos esos archivos y se nos irán abriendo tabs.



## Limpiar metadatos de archivos :

Una vez tenemos extraídos los metadatos, si es que queremos limpiar el documento de estos, solo tenemos que dar al botón “clear selected” para borrar los metadatos del documento seleccionado o “clear all” para borrar todos los metadatos de todos los archivos abiertos.

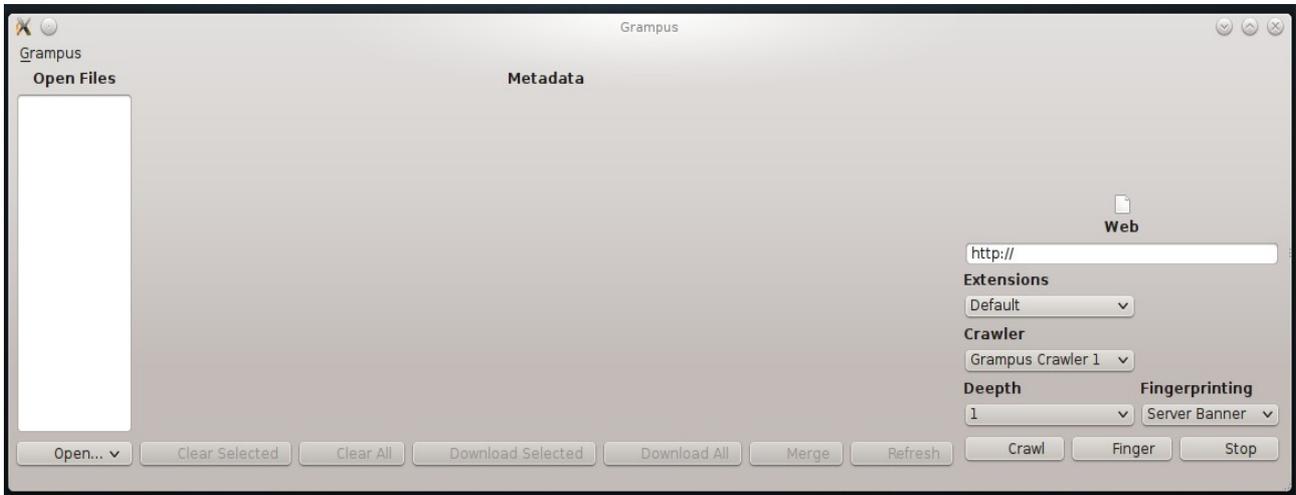
Una vez clickearas sobre el botón de limpiar, al comprobar el directorio en el que se encontraba el/los documento/s nos encontraremos con que hay otro archivo con el mismo nombre pero con una ligera diferencia, el sufijo “CLEANED”.



Limpio...

## Uso de los crawlers :

Para poder hacer uso de los crawlers deberemos desplazarnos al botón “open” y seleccionar la opción “url”, un nuevo panel se nos abra en la GUI :



### Crawlers :

- Grampus crawler 1
- Grampus crawler 2
- Google
- Bing

### Grampus Crawler 1:

Escribimos el url de la web que vamos a crawlear en el input, seleccionamos Grampus Crawler 1 como crawler, dejamos la profundidad por default en este caso y clickeamos en el botón “Crawl” para empezar a crawlear el sitio, el crawler nos generará una serie de reportes en html, donde podremos apreciar el reporte de una manera mucho más cómoda.

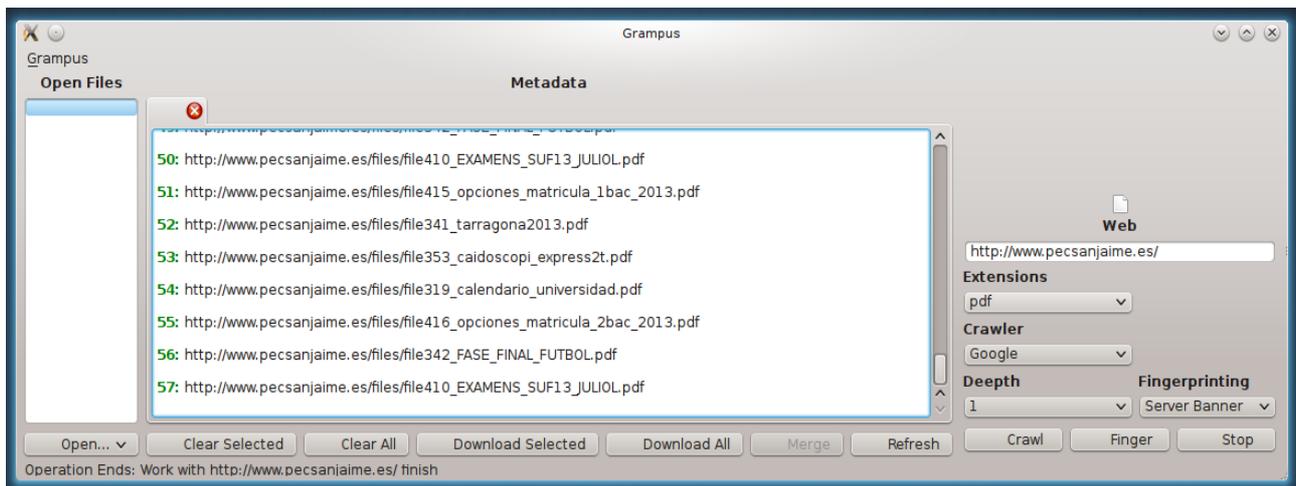
### Grampus Crawler 2:

Actualmente inactivo

### Google :

Escribimos el url del website que vamos a crawlear en el input, seleccionamos la extensión del documento público que queremos extraer de la web objetivo, en caso de que querramos extraer documentos públicos, seleccionamos “Google” como Crawler y clickeamos en “Crawl”

Se nos abrirá un tab en el que apareceran numerados todos los pdf's encontrados en el website, posteriormente podremos descargarlos uno a uno (Download Selected) para su análisis o descargarlos todos (Download All).



Bing :

Actualmente inactivo

## Uso de las tareas de fingerprinting :

Para poder dar uso de las funciones fingerprinting implementadas en Grampus, debemos escribir la url del site que queremos escanear y seleccionamos :

- Server banner
- Shodan
- Port Scanner (inactivo)
- Sniffer (inactivo)

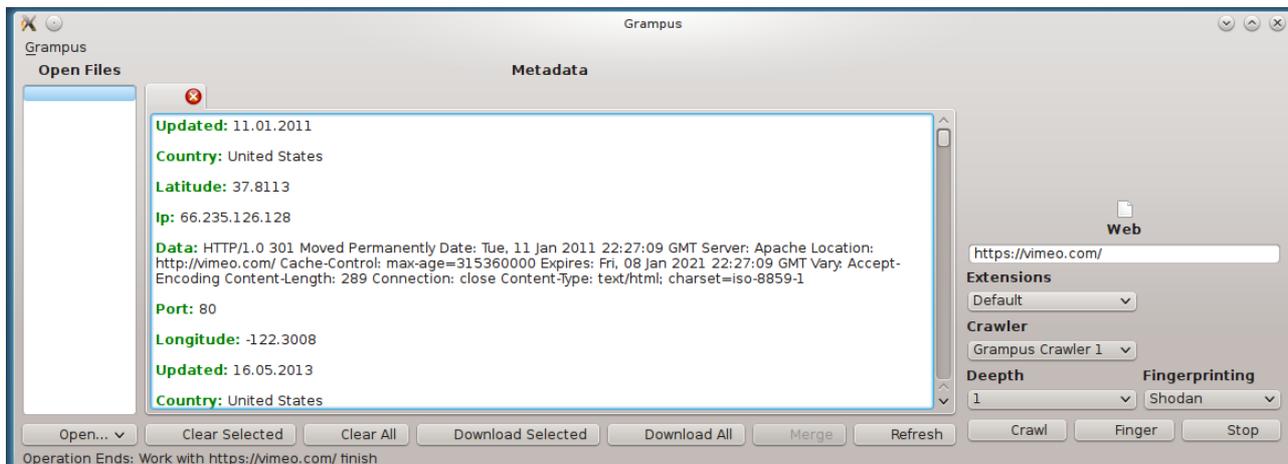
## Server Banner :



Proceso para extraer información del server, como lenguaje, tipo de servidor, hora del servidor, etc...

## Shodan

Utiliza la api de shodan para realizar un escaneo al website objetivo y sacar información acerca de él.



Esto es todo lo que consideramos que debeis hacer para comenzar a usar el software aunque de por si solo es muy intuitivo.