GRAMPUS - GUÍA DE USUARIO

Índice :

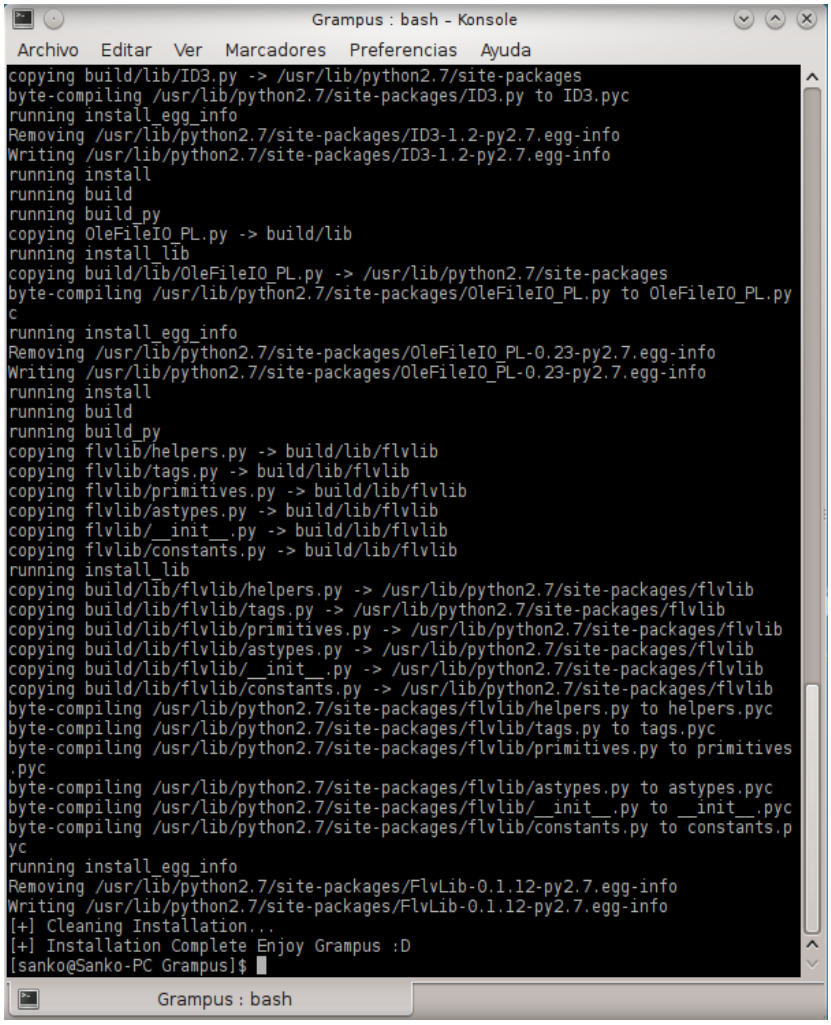
- Instalación
- Ejecución
- Extraer metadatos de archivos
- Limpiar metadatos de archivos
- Uso de los crawlers
- Uso de las tareas de fingerprinting

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.



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 librerias.

Ejecución :

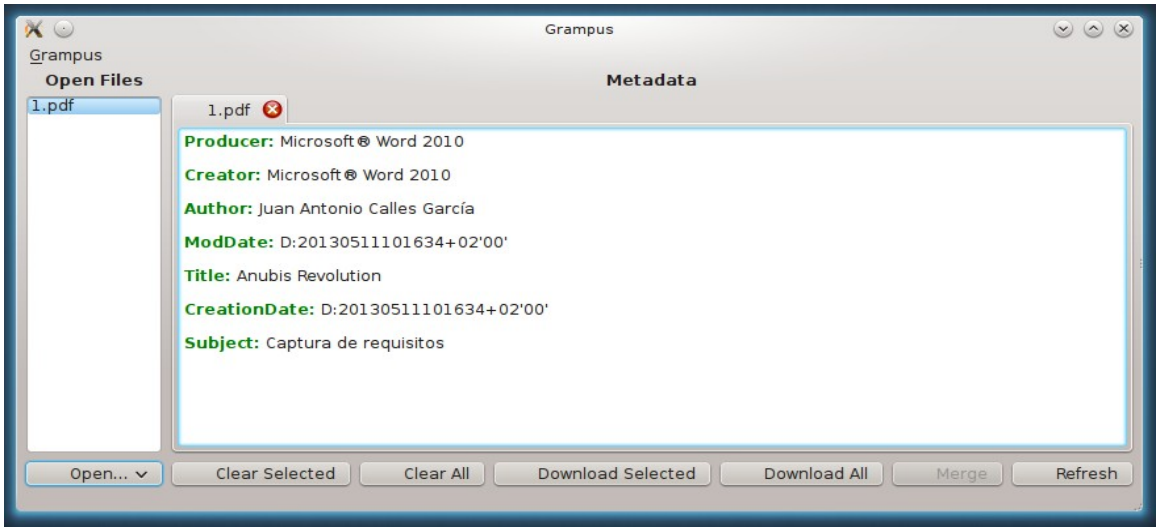
Una vez ya tenemos las dependencias instaladas podemos pasar a la ejecución de la GUI, escribimos en terminal/cmd :

python MainGrampus.py

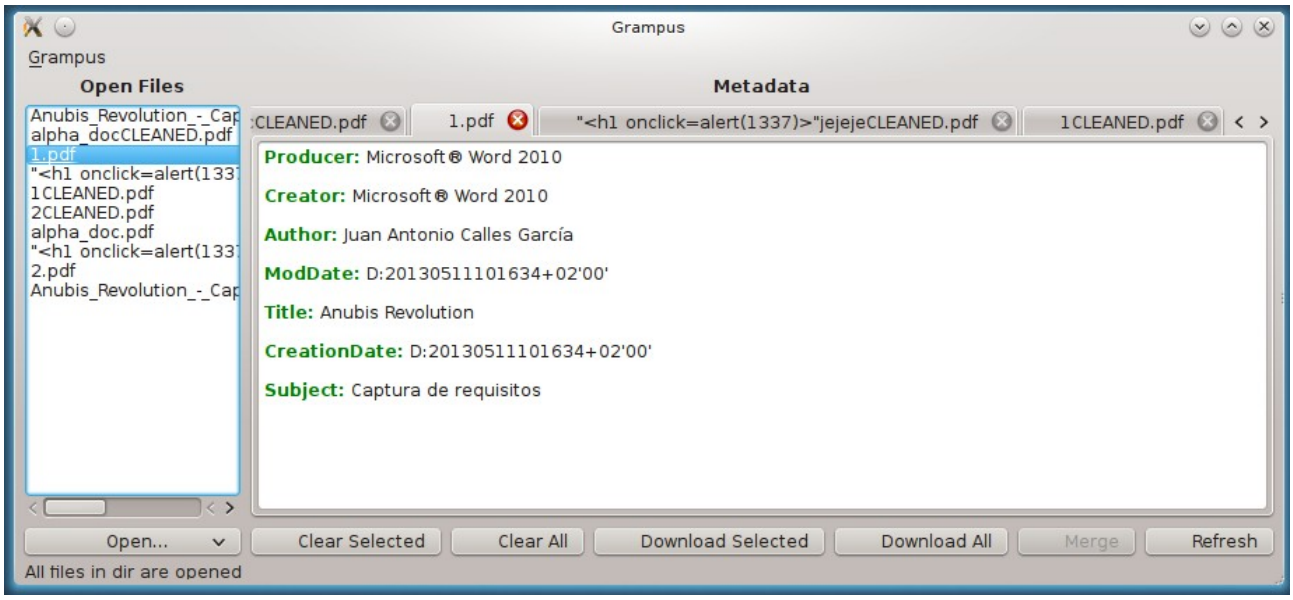
y se nos abrirá la interfaz gráfica :

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.



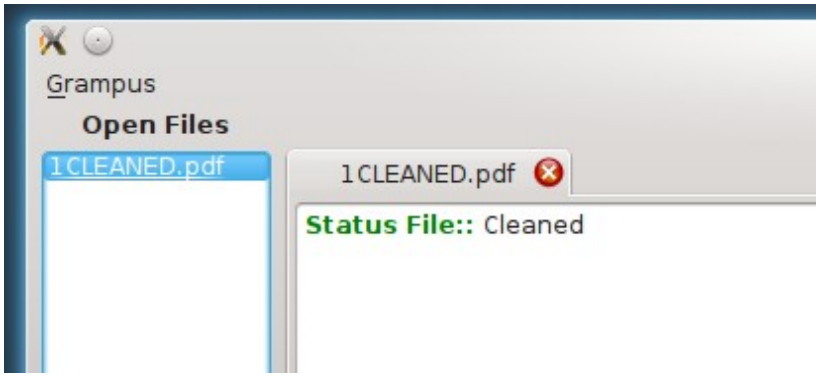
· **<u>Directorios</u> :**
Para extraerlos metadatos de todos los archivos contenidos en un directorio, solo tenemos que desplazarnos hasta el botón “Open” > “Directory”, una vez hecho esto seleccionamos el directorio en el que tenemos contenidos todos esos archivos y se nos iran abriendo tabs.



<u>Limpiar metadatos de archivos</u> :

Una vez tenemos extraidos 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 abrira 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.

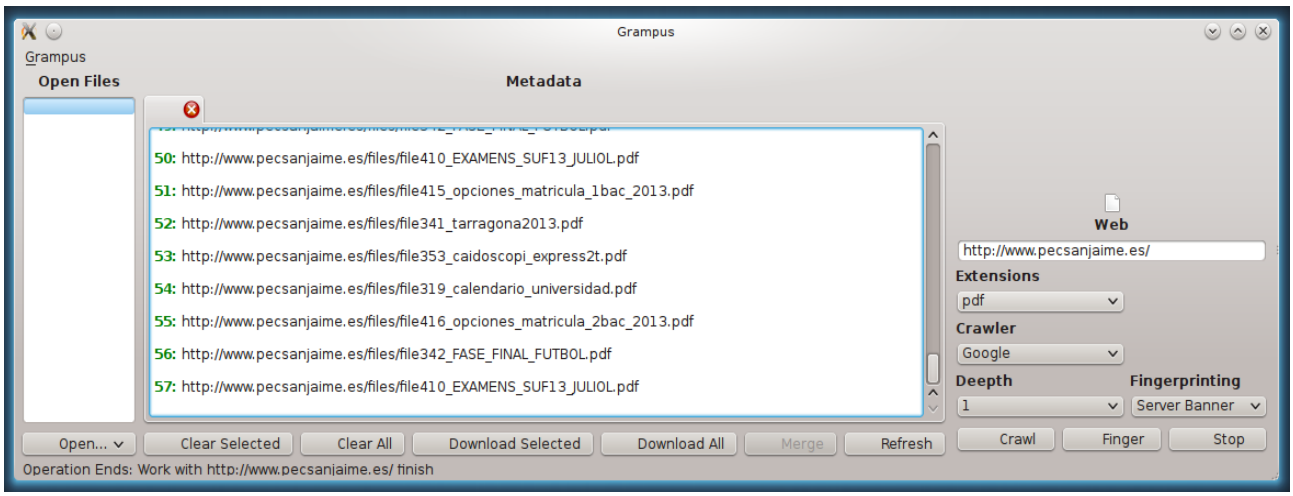
Grampus Crawler 2:

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).



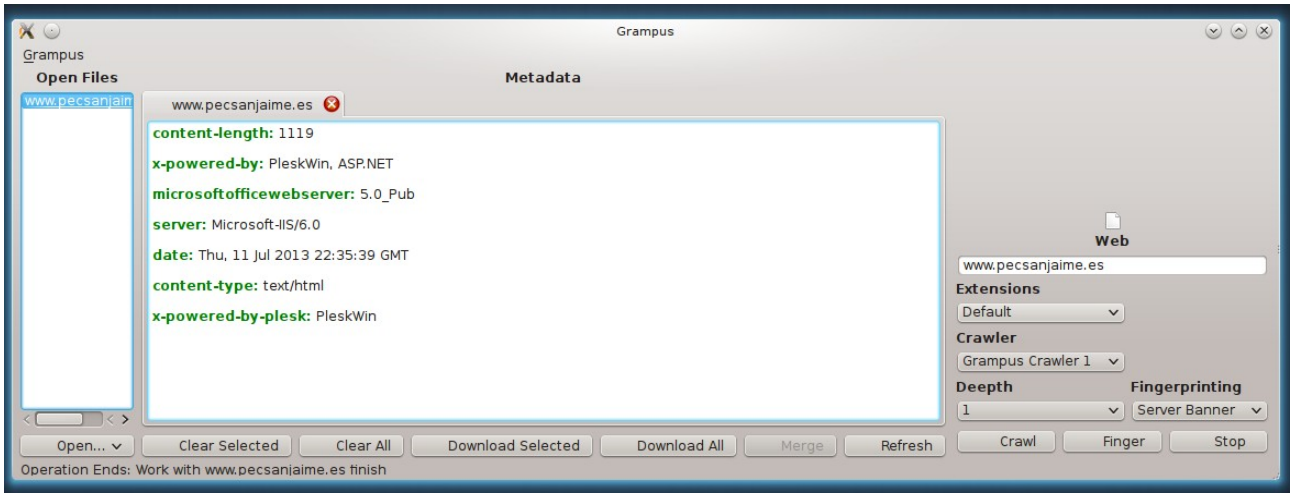
Bing :
Actualmente inactivo

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)

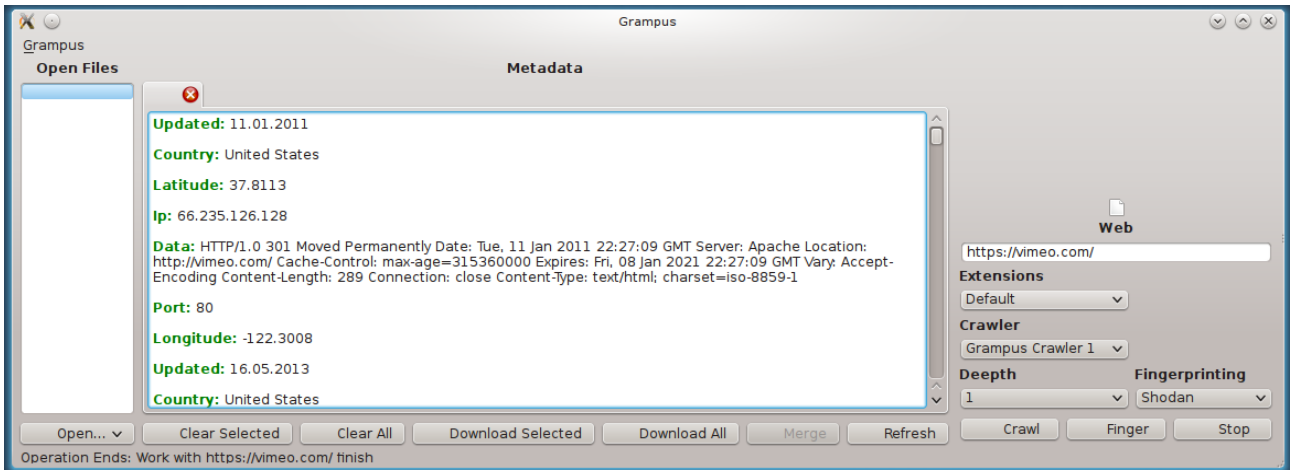
Server Banner :



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.