

Documentación

on

Navegación

Pia Pc

- Contenido:
- Main (PIA)
- Script del Main
- Scan
- Script del Scan
- Hash
- Script del Hash
- Meta
- Script del Meta
- Scrap
- Script del Scrap
- Correo
- Script del Correo
- Script de Power Shell
- Requirements

Búsqueda rápida

[Ira](#)

Pia Pc

Integrantes:

Jared Abraham Perez Guerrero. 1863721

Felipe De Jesus Mares Mojica. 1924831

Jose Osvaldo Puga Leija. 1990132

Contenido:

- Main (PIA)
- Script del Main
- Scan
- Script del Scan
- Hash
- Script del Hash
- Meta
- Script del Meta
- Scrap
- Script del Scrap
- Correo
- Script del Correo
- Script de Power Shell
- Requirements

Main (PIA)

Este es el código principal de nuestro script, es el que tiene todos los procesos de los demás scripts unificados para una ejecución más rápida y cómoda para el usuario Tiene dos funciones distintas por medio de algunos parámetros de argparse El primero es una instrucción para analizar un enlace por medio de otro script utilizando un api de virus total, hacerle un poco de webscrapping y obtener los metadatos a las imágenes La instrucción de uso es la siguiente: PIA.py -link (link a analizar) -a (introduce su api key de virustotal) La otra instrucción es acerca de sacar el valor hash de un directorio de archivos y mandarle esa información a alguien por medio de un correo electrónico La instrucción de uso es la siguiente PIA.py -b (nombre del archivo pickle) -p (dirección path a analizar) -t (nombre del txt con los hashes ordenados).txt -u (correo desde donde se mandara) -w (contraseña de su correo) -y (correo destinatario)

Script del Main



Scan

Este código utiliza la api de virustotal para escanear un link buscando código malicioso dentro, además de generar un reporte para el usuario.

Script del Scan



Hash

En este script, se importan dos módulos característicos de Python, el subprocess que nos sirve para generar procesos adicionales y aunado a la función run() nos ejecuta un comando externo sin interactuar con el, también incluye funciones de powershell como sellstddo que nos indica si el registro de errores de powershell no nos indica error nos imprimirá lo que viene a continuación, después viene una sección de open tmpfile que nos creara un archivo temporal donde se imprimirá el valor hash de los archivos que fueron especificados dando un formato de líneas separadas por subcadenas donde en la posición 0 nos imprimirá el valor hash, y en la 1 se imprimirá el nombre del archivo. Después el código tiene un apartado donde nos lee un archivo con permiso de escritura lo pasara como diccionario y después muestra en pantalla datos del archivo, finalmente usamos la función pickle.dump. Después, función para almacenar los datos del objeto en el archivo. La función pickle.dump () que toma 3 argumentos. El primer argumento es el objeto que desea almacenar. El segundo argumento es el objeto de archivo que obtiene al abrir el archivo deseado en modo de escritura binaria (wb). Y el tercer argumento es el argumento clave-valor. Este argumento define el protocolo. Y al final del script, nos arroja los errores en caso de presentarse

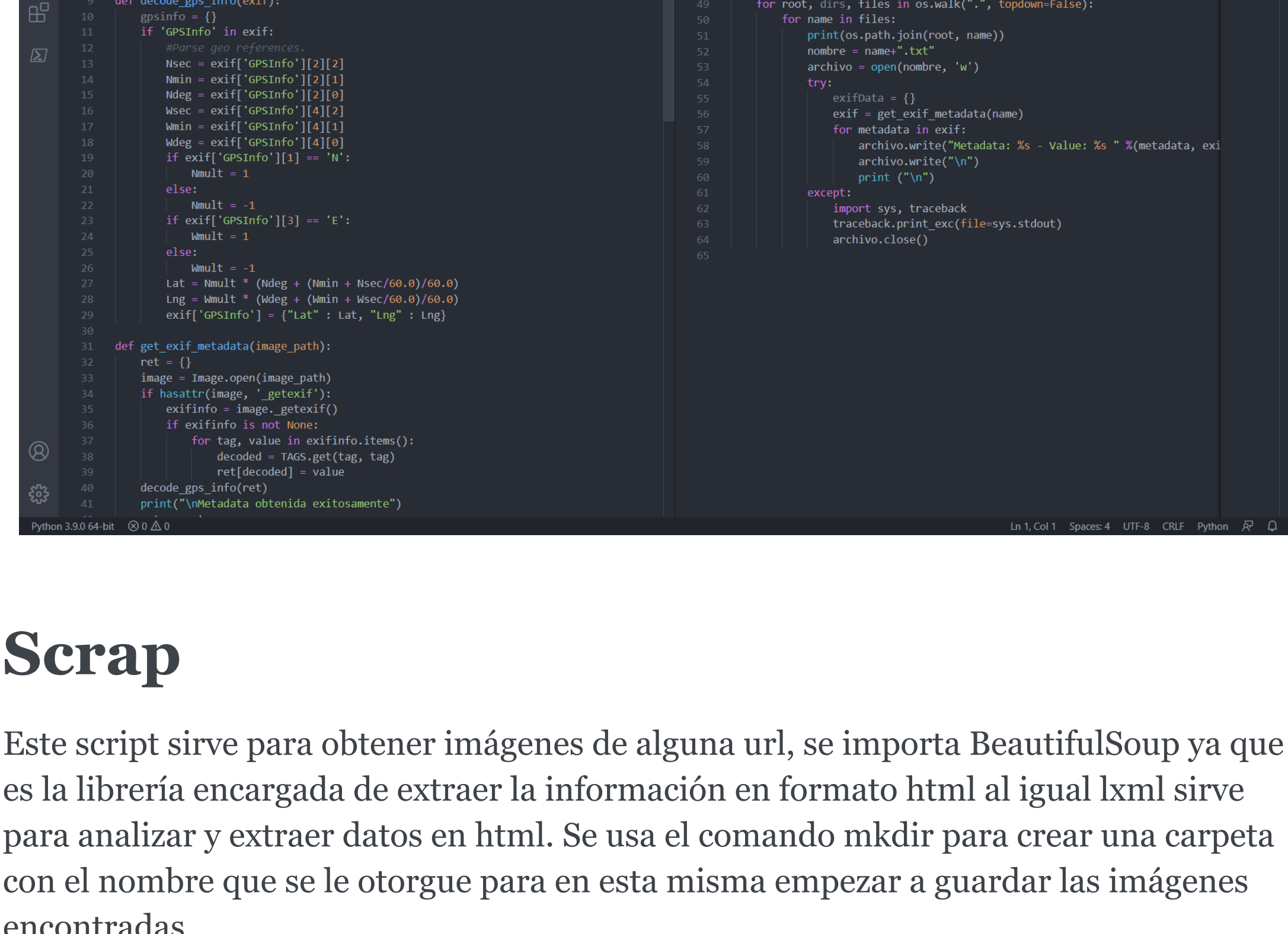
Script del Hash



Meta

El módulo argparse facilita la escritura de interfaces de línea de comandos fáciles de usar. El programa define qué argumentos requiere y argparse descubrirá cómo analizarlos sys.argv. El argparse módulo también genera automáticamente mensajes de ayuda y uso y emite errores cuando los usuarios dan al programa argumentos no válidos El módulo Requests es un módulo de Python que puedes usar para enviar todo tipo de peticiones HTTP. Es una librería muy fácil de usar con muchas características variando desde pasar parámetros en URLs. El módulo (PIL) es una librería gratuita que permite la edición de imágenes directamente desde Python. Y finalmente, BeautifulSoup nos permite hacer el webscrapping y acomodarlo de una manera amigable. Las líneas a esta orientada a la obtención de los metadatos de interés, en este caso se trata de los datos de geolocalización o coordenadas de la imagen, también tenemos líneas como hashr que, toma como argumentos un objeto y el nombre de un atributo y retorna True si el objeto contiene dicho atributo, dando paso a la siguiente parte del script que es la obtención de metadatos. Después Se imprime caracteres de nueva línea como parte de la salida en la terminal con la línea archivo.write(«\n»), finalmente con la línea traceback.print_exc(file=sys.stdout), nos vamos a la última parte que es un seguimiento de la pila desde el punto de un controlador de excepciones en la cadena de llamadas hasta el punto donde se generó la excepción, en este caso se imprimirá dicha información.

Script del Meta



Scrap

Este script sirve para obtener imágenes de alguna url, se importa BeautifulSoup ya que es la librería encargada de extraer la información en formato html al igual lxml sirve para analizar y extraer datos en html. Se usa el comando mkdir para crear una carpeta con el nombre que se le otorgue para en esta misma empezar a guardar las imágenes encontradas.

Script del Scrap



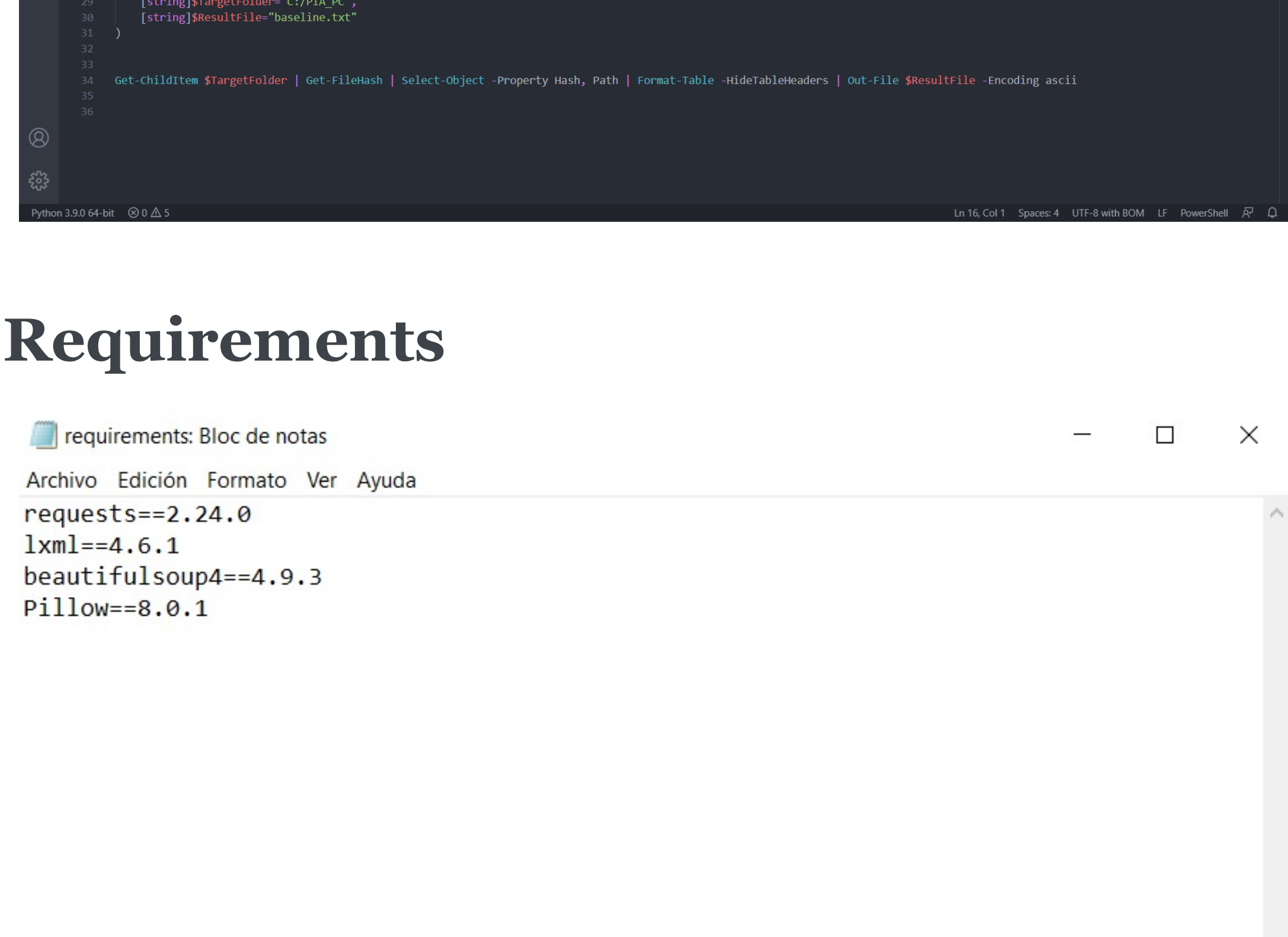
Correo

Este script sirve para mandar un correo con un archivo adjunto es un modulo en el cual se puede usar para enviar un correo electrónico a cualquier máquina de internet y se importa MIME para poder adjuntar archivos de texto se usa la variable smtpServer la cual es el protocolo indicado para poder mandar estos correos. Y ya al momento de ejecutarlo te pido el usuario contraseña el archivo con el path de donde está ubicado y al correo que se le mandara el archivo.


Script del Correo



Script de Power Shell



Requirements

 requirements: Bloc de notas	—	□	×
Archivo Edición Formato Ver Ayuda			
requests==2.24.0			
lxml==4.6.1			
beautifulsoup4==4.9.3			
Pillow==8.0.1			
Línea 1, columna 1			
100%			
Windows (CRLF)			
UTF-8			