

## **Producto Integrador de Aprendizaje**



### **Instrucciones de uso**

**Creado por:**

Julia Fernanda Ramírez Oviedo

Silvestre Martínez Cervantes

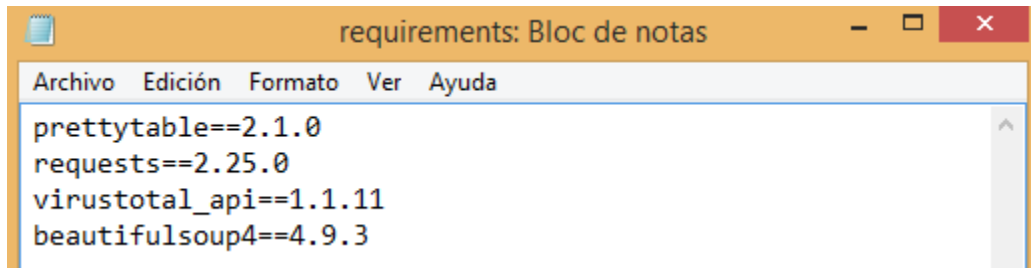
## Información general

Este proyecto realiza 5 tareas relacionadas con la ciberseguridad. Las tareas que realiza son las siguientes:

- 1) Obtención de hash.
- 2) Escaneo de puertos.
- 3) Análisis de ejecutables.
- 4) Web Scraping.
- 5) Estatus de procesos y servicios.

## Requisitos

-Instalar todos los módulos necesarios que están en el archivo requirements.txt para que los scripts funcionen.



```
prettytable==2.1.0
requests==2.25.0
virustotal_api==1.1.11
beautifulsoup4==4.9.3
```

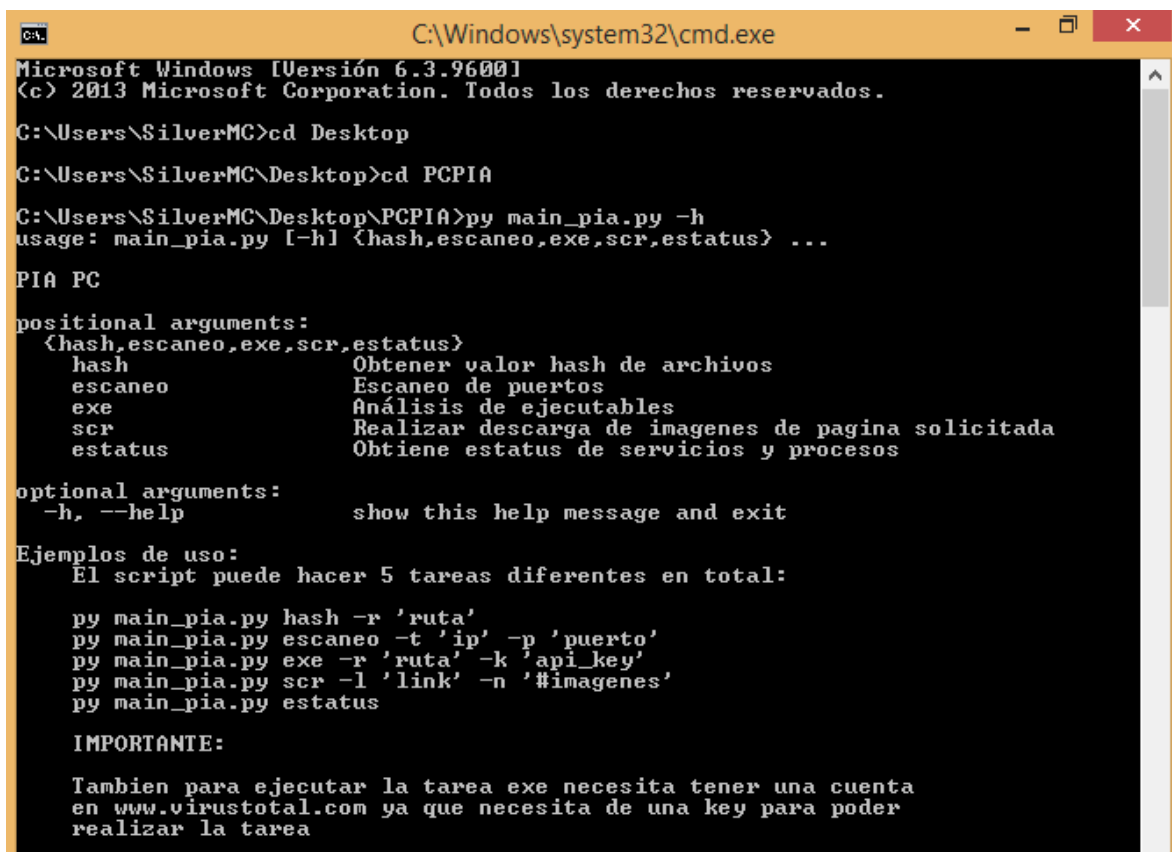
-Tener Python 3 instalado.

-Tener Powershell versión 4.0 en adelante instalado.

## Instrucciones

El script que se debe ejecutar es el `main_pia.py`, para eso necesitamos hacerlo desde la Shell de Windows ya que funciona con el módulo `argparse` y necesita parámetros para poder funcionar correctamente.

-h: Esta opción nos mostrará información de ayuda para ejecutar el script correctamente.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.

C:\Users\SilverMC>cd Desktop
C:\Users\SilverMC\Desktop>cd PCPIA
C:\Users\SilverMC\Desktop\PCPIA>py main_pia.py -h
usage: main_pia.py [-h] {hash,escaneo,exe,scr,estatus} ...

PIA PC

positional arguments:
  {hash,escaneo,exe,scr,estatus}
    hash                Obtener valor hash de archivos
    escaneo              Escaneo de puertos
    exe                  Análisis de ejecutables
    scr                  Realizar descarga de imagenes de pagina solicitada
    estatus              Obtiene estatus de servicios y procesos

optional arguments:
  -h, --help            show this help message and exit

Ejemplos de uso:
  El script puede hacer 5 tareas diferentes en total:

  py main_pia.py hash -r 'ruta'
  py main_pia.py escaneo -t 'ip' -p 'puerto'
  py main_pia.py exe -r 'ruta' -k 'api_key'
  py main_pia.py scr -l 'link' -n '#imagenes'
  py main_pia.py estatus

  IMPORTANTE:

  Tambien para ejecutar la tarea exe necesita tener una cuenta
  en www.virustotal.com ya que necesita de una key para poder
  realizar la tarea
```

Para obtener información de cada tarea, escribir lo siguiente:

`py main_pia.py 'tarea' -h`

## 1) hash - Obtención de hash

Esta tarea nos permite obtener valor hash de archivos.

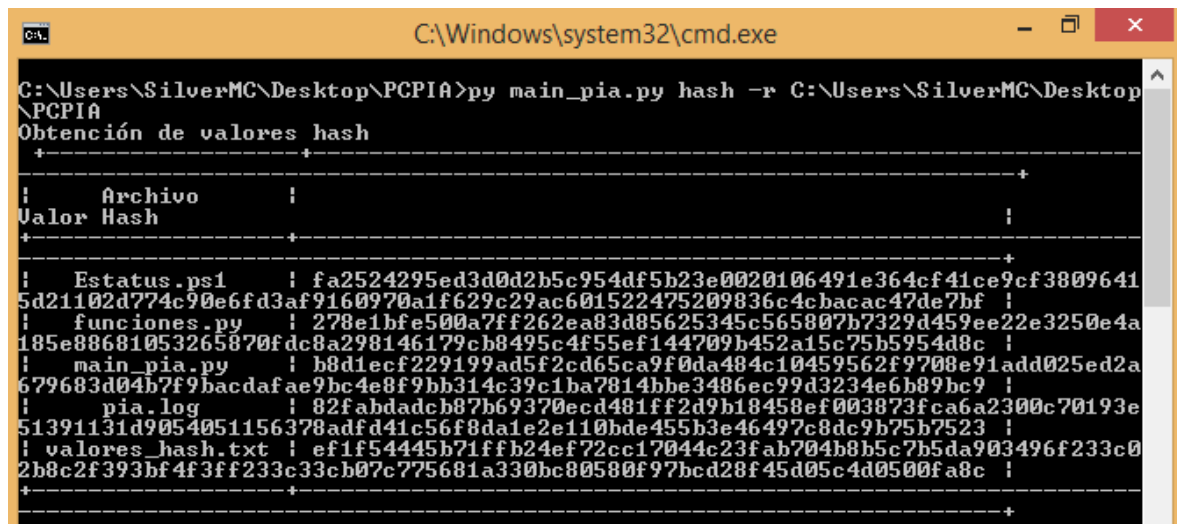
Para ejecutar la tarea hay que escribir lo siguiente:

```
py main_pia.py hash -r 'ruta'
```

-r: Ingresar una ruta en la cual queremos ver el valor hash de su contenido.

Por ejemplo:

```
py main_pia.py hash -r C:\Users\SilverMC\Desktop\PCPIA
```



```
C:\Windows\system32\cmd.exe
C:\Users\SilverMC\Desktop\PCPIA>py main_pia.py hash -r C:\Users\SilverMC\Desktop\PCPIA
Obtención de valores hash
+-----+
| Archivo | Valor Hash |
+-----+-----+
| Estatus.ps1 | fa2524295ed3d0d2b5c954df5b23e0020106491e364cf41ce9cf38096415d21102d774c90e6fd3af9160970a1f629c29ac601522475209836c4cbacac47de7bf |
| funciones.py | 278e1bfe500a7ff262ea83d85625345c565807b7329d459ee22e3250e4a185e88681053265870fdc8a298146179cb8495c4f55ef144709b452a15c75b5954d8c |
| main_pia.py | b8d1ecf229199ad5f2cd65ca9f0da484c10459562f9708e91add025ed2a679683d04b7f9bacdafae9bc4e8f9bb314c39c1ba7814bbe3486ec99d3234e6b89bc9 |
| pia.log | 82fabdadcb87b69370ecd481ff2d9b18458ef003873fca6a2300c70193e51391131d9054051156378adfd41c56f8da1e2e110bde455b3e46497c8dc9b75b7523 |
| valores_hash.txt | ef1f54445b71ffb24ef72cc17044c23fab704b8b5c7b5da903496f233c02b8c2f393bf4f3ff233c33cb07c775681a330bc80580f97bcd28f45d05c4d0500fa8c |
+-----+-----+
```

Una vez ejecutado la instrucción, se generará un archivo llamado valores\_hash.txt con los valores hash de los archivos.

Nombre	Fecha de modifica...	Tipo	Tamaño
__pycache__	14/05/2021 08:25 ...	Carpeta de archivos	
Estatus	13/05/2021 10:11 a...	Script de Window...	1 KB
funciones	14/05/2021 05:07 ...	Python File	7 KB
main_pia	14/05/2021 07:31 ...	Python File	7 KB
pia	14/05/2021 08:25 ...	Documento de tex...	2 KB
valores_hash	14/05/2021 08:25 ...	Documento de tex...	1 KB

También puedes ejecutar la instrucción especificando si solo quieres el valor hash de un archivo, por ejemplo:

```
py main_pia.py hash -r C:\Users\SilverMC\Desktop\PCPIA\funciones.py
```

## 2) escaneo – Escaneo de puertos

Esta tarea nos permite saber si tenemos puertos abiertos o cerrados de cierta ip.

Para ejecutar la tarea hay que escribir lo siguiente:

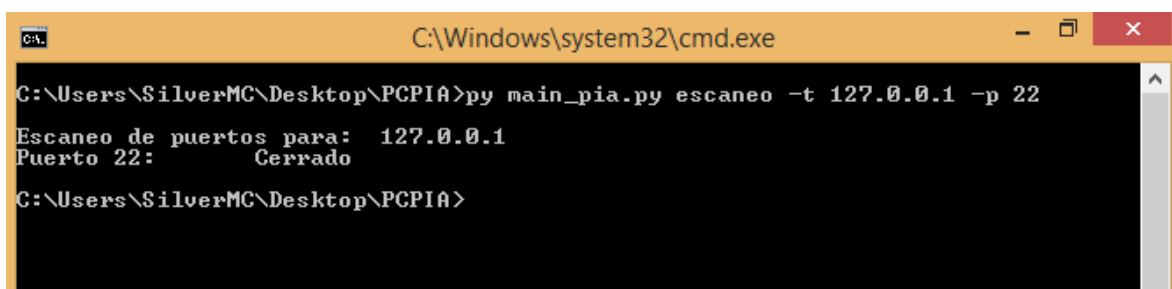
```
py main_pia.py escaneo -t 'ip' -p 'puerto'
```

-t: Ingresar una ip. Se puede ingresar varias ip's separadas por comas. Este argumento es opcional, por lo que, si no se ingresa, por default tendrá el valor de "127.0.0.1".

-p: Ingresar el puerto a analizar Se puede ingresar un rango de puertos a analizar separados por una coma. Ej: -p 22,100

Por ejemplo:

```
py main_pia.py escaneo -t 127.0.0.1 -p 22
```



```
C:\Windows\system32\cmd.exe

C:\Users\SilverMC\Desktop\PCPIA>py main_pia.py escaneo -t 127.0.0.1 -p 22
Escaneo de puertos para: 127.0.0.1
Puerto 22: Cerrado

C:\Users\SilverMC\Desktop\PCPIA>
```

Una vez ejecutado la instrucción, se generará un archivo llamado Escaneo\_IP.txt con la información de los puertos de la ip ingresada.

Nombre	Fecha de modifica...	Tipo	Tamaño
__pycache__	14/05/2021 08:34 ...	Carpeta de archivos	
Escaneo_IP	14/05/2021 08:39 ...	Documento de tex...	1 KB
Estatus	13/05/2021 10:11 a...	Script de Window...	1 KB
funciones	14/05/2021 05:07 ...	Python File	7 KB
main_pia	14/05/2021 07:31 ...	Python File	7 KB
pia	14/05/2021 08:39 ...	Documento de tex...	1 KB

### 3) exe - Análisis de ejecutables

Esta tarea nos permite saber si archivo .exe es un archivo seguro o malicioso.

Para ejecutar la tarea hay que escribir lo siguiente:

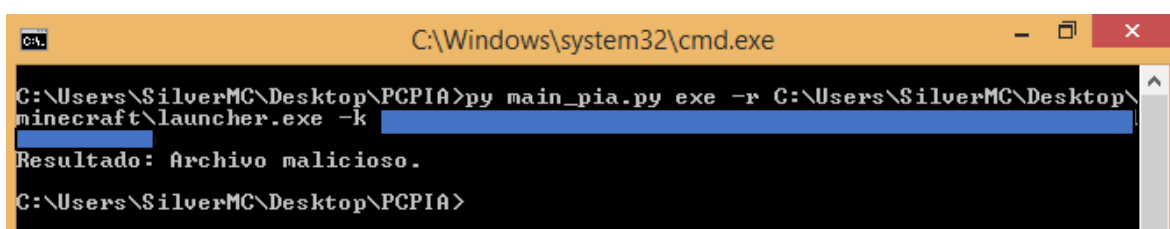
```
py main_pia.py exe -r 'ruta' -k 'api_key'
```

-r: Ingresar la ruta donde se encuentre el ejecutable.

-k: Ingresar una api key. Para obtenerla, es necesario tener una cuenta en [www.virustotal.com](https://www.virustotal.com).

Por ejemplo:

```
py main_pia.py exe -r C:\Users\SilverMC\Desktop\minecraft\launcher.exe -k 'api_key'
```



```
C:\Windows\system32\cmd.exe
C:\Users\SilverMC\Desktop\PCPIA>py main_pia.py exe -r C:\Users\SilverMC\Desktop\minecraft\launcher.exe -k [redacted]
Resultado: Archivo malicioso.
C:\Users\SilverMC\Desktop\PCPIA>
```

Una vez ejecutado la instrucción, se generará un archivo llamado rep\_exe.txt con el resultado obtenido del archivo.

Nombre	Fecha de modifica...	Tipo	Tamaño
__pycache__	14/05/2021 08:34 ...	Carpeta de archivos	
Estatus	13/05/2021 10:11 a...	Script de Window...	1 KB
funciones	14/05/2021 05:07 ...	Python File	7 KB
main_pia	14/05/2021 07:31 ...	Python File	7 KB
pia	14/05/2021 09:18 ...	Documento de tex...	2 KB
rep_exe	14/05/2021 09:02 ...	Documento de tex...	1 KB

#### 4) scr – Web scraping

Esta tarea nos permite descargar imágenes de una página web.

Para ejecutar la tarea hay que escribir lo siguiente:

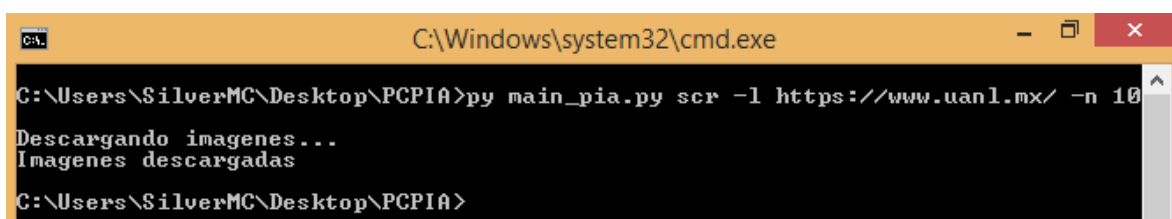
```
py main_pia.py scr -l 'link' -n '#imagenes'
```

-l: Ingresar el link de la página a hacer web scraping.

-n: Ingresar el número de imágenes a descargar.

Por ejemplo:

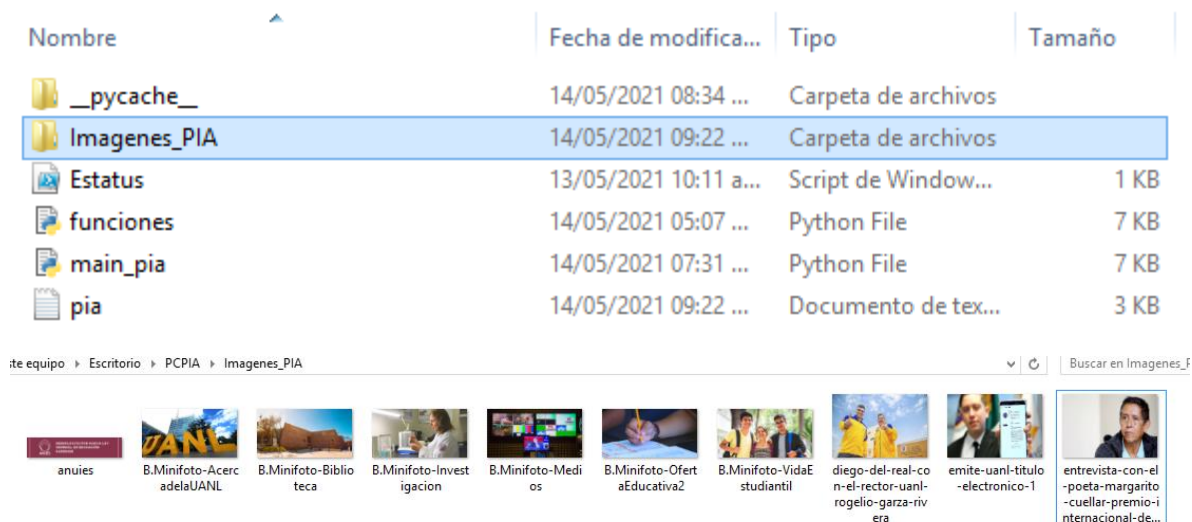
```
py main_pia.py scr -l https://www.uanl.mx/ -n 10
```



```
C:\Windows\system32\cmd.exe

C:\Users\SilverMC\Desktop\PCPIA>py main_pia.py scr -l https://www.uanl.mx/ -n 10
Descargando imagenes...
Imagenes descargadas
C:\Users\SilverMC\Desktop\PCPIA>
```

Una vez ejecutado la instrucción, se generará una carpeta llamada Imagenes\_PIA con las imágenes descargadas.



## 5) estatus - Estatus de procesos y servicios

Esta tarea nos permite ver que servicios del sistema se están ejecutando, cuales están detenidos y también nos permite ver información de los procesos del sistema que se están ejecutando.

Para ejecutar la tarea hay que escribir lo siguiente:








```
py main_pia.py estatus
```

```
wscntfrg is Running
WSearch is Running
WSService is Stopped
wuauserv is Stopped
wudfsvc is Running
WwanSvc is Stopped
ZeroConfigService is Running
La transcripción se ha detenido. El archivo de salida es C:\Users\SilverMC\Desktop\PCPIA\Servicios.txt

===INFORMACION DE PROCESOS===
La transcripción ha comenzado. El archivo de salida es C:\Users\SilverMC\Desktop\PCPIA\Procesos.txt
```

Handles	NPM(K)	PM(K)	WS(K)	UM(M)	CPU(s)	Id	ProcessName
284	20	5048	11304	129	2.58	4336	AAAM Updates Notifier
82	9	1224	4268	72	0.08	1480	acrotray
36	4	512	2132	12		1628	AERTSr64
74	7	1024	3324	74		1608	armsvc
185	12	2264	6484	94		576	atieclxx
114	6	812	2820	22		932	atiesrxx
109	10	1560	5032	86	0.17	6516	atiw
170	12	8432	13768	0	0.69	4000	audiodg
735	52	111896	5356	843	12.14	7148	CCC
474	29	220724	244352	0	180.14	348	chrome
191	12	12848	15596	0	4.77	1008	chrome

Una vez ejecutado la instrucción, se generará dos archivos llamados Servicios.txt y Procesos.txt en donde se guardará la información mostrada en pantalla.

Nombre	Fecha de modifica...	Tipo	Tamaño
 __pycache__	14/05/2021 08:34 ...	Carpeta de archivos	
 Estatus	13/05/2021 10:11 a...	Script de Window...	1 KB
 funciones	14/05/2021 05:07 ...	Python File	7 KB
 main_pia	14/05/2021 07:31 ...	Python File	7 KB
 pia	14/05/2021 09:27 ...	Documento de tex...	7 KB
 Procesos	14/05/2021 09:27 ...	Documento de tex...	8 KB
 Servicios	14/05/2021 09:27 ...	Documento de tex...	5 KB



## pia.log

Este archivo registra todas las acciones que suceden a la hora de ejecutar una tarea del script, así como los errores que puedan ocurrir.

```
Archivo Edición Formato Ver Ayuda
INFO:root:https://www.uanl.mx/wp-content/uploads/2018/12/8.Minifoto-Investigacion.jpg descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2018/12/8.Minifoto-Biblioteca.jpg descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2018/12/8.Minifoto-Medios.jpg descargando...
INFO:root:https://www.uanl.mx/wp-content/themes/uanl/assets/img/logotipo-U.png descargando...
INFO:root:https://www.uanl.mx/wp-content/themes/uanl/assets/img/logotipo-U.png descargando...
INFO:root:https://www.uanl.mx/wp-content/themes/uanl/assets/img/logotipo-U.png descargando...
INFO:root:https://www.uanl.mx/wp-content/themes/uanl/assets/img/logotipo-U.png descargando...
INFO:root:https://www.uanl.mx/wp-content/themes/uanl/assets/img/logotipo-U.png descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2021/05/entrevista-con-el-poeta-margarito-cuellar-premio-internacional-de-poesia-pilar-fernandez-labador-3-1.jpg desc
INFO:root:https://www.uanl.mx/wp-content/uploads/2021/05/visita-secretaria-educacion-publica-delfina-gomez-vacunacion-covid19-fime-uanl-rector-rogelio-garza-1.jpg desc
INFO:root:https://www.uanl.mx/wp-content/uploads/2021/05/etrevista-dra-maria-luisa-martinez-directora-del-iinso-20-aniversario-del-iinso-1-1.jpg descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2021/05/entrevista-paola-marmolejo-agresada-uanl-exposicion-creadora-mujeres-artistas-1-1.jpg descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2021/05/festival-alfonsino-uanl-2021-1.jpg descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2021/05/diego-del-real-con-el-rector-uanl-rogelio-garza-rivera.jpg descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2021/01/uanl-2021.jpg descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2020/08/recomendaciones-covid19.jpg descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2021/01/emite-uanl-titulo-electronico-1.jpg descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2020/06/protocolo-prevencion.jpg descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2021/04/anuies.jpg descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2021/01/Intercambio-Internacional-1.jpg descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2021/02/RAC-UANL.jpg descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2019/01/VideoInstitucional.jpg descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2019/01/OfertaEducativa.jpg descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2020/12/Sorteo-de-la-siembra.jpg descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2020/08/Escudo-UANL-color.png descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2020/08/Vision2030-color.png descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2020/08/logo-contraloria-2020.jpg descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2021/01/PremioOX.png descargando...
INFO:root:https://www.uanl.mx/wp-content/uploads/2019/03/logotipo-somos-uni.png descargando...
INFO:root:https://www.uanl.mx/ Imagenes descargadas
INFO:root:Ejecutando Estatus.ps1
INFO:root:Procesos.txt generado
INFO:root:Servicios.txt generado
ERROR:root:Ha ocurrido un error: Invalid URL 'paginaInexistente.com': No schema supplied. Perhaps you meant http://paginaInexistente.com?
```