

## PRÁCTICA RECOPIACIÓN INFORMACIÓN

Empresa elegida: SHOPIFY.COM, es una plataforma para crear una ecommerce. Te permite crear una tienda online, puedes personalizarla, vender productos en cualquier país del mundo. Tiene un amplio catálogo de productos.

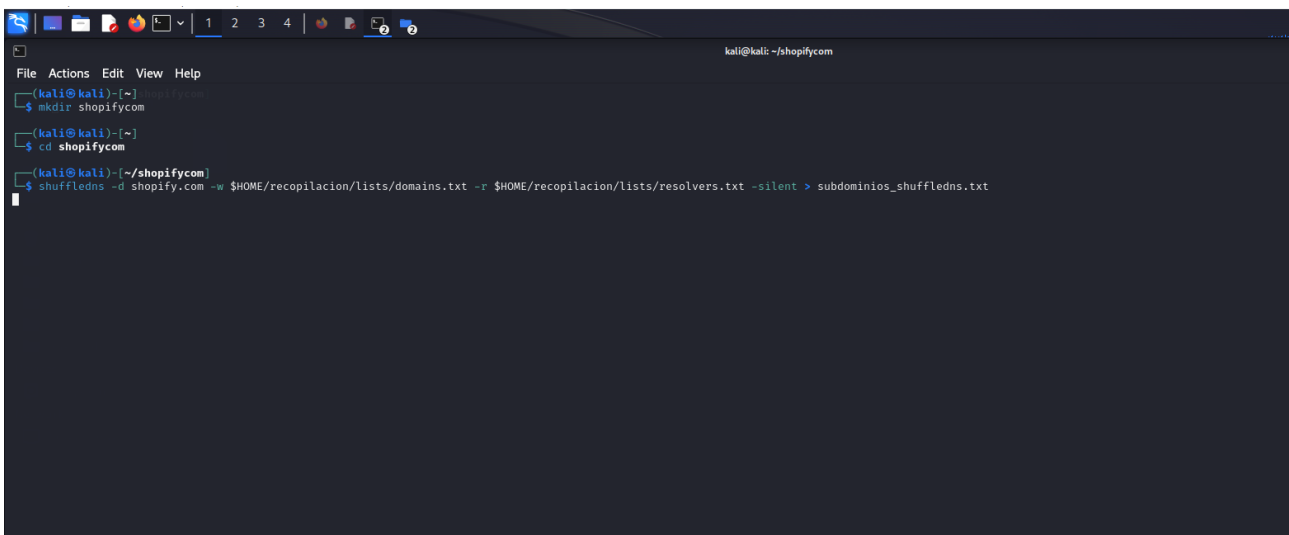
Reconocimiento en 2 fases: FOOTPRINTING y FINGERPRINTING

FOOTPRINTING:

Herramientas y comandos utilizados:

SHUFFLEDNS, sirve para encontrar subdominios a través de peticiones DNS. Ejecutamos el comando:

```
shuffledns -d shopify.com -w $HOME/recopilacion/lists/domains.txt -r $HOME/recopilacion/lists/resolvers.txt -silent > subdominios_shuffledns.txt
```

A screenshot of a Kali Linux terminal window. The window title is 'kali@kali: ~/shopifycom'. The terminal shows the following commands and their outputs:  
1. Prompt: (kali@kali)-[~]  
Command: \$ mkdir shopifycom  
Output: (kali@kali)-[~]  
2. Prompt: (kali@kali)-[~]  
Command: \$ cd shopifycom  
Output: (kali@kali)-[~/shopifycom]  
3. Prompt: (kali@kali)-[~/shopifycom]  
Command: \$ shuffledns -d shopify.com -w \$HOME/recopilacion/lists/domains.txt -r \$HOME/recopilacion/lists/resolvers.txt -silent > subdominios\_shuffledns.txt  
The terminal is dark-themed with a light blue prompt and command text. The output of the shuffledns command is not visible in the screenshot.

vemos en el fichero subdominios\_shuffledns.txt el contenido de lo que hemos obtenido:



y obtenemos:

```
File Actions Edit View Help
(kali㉿kali)-[~/shopifycom]
$ analyticsrelationships --url shopify.com

UA-ID
DOMAINS

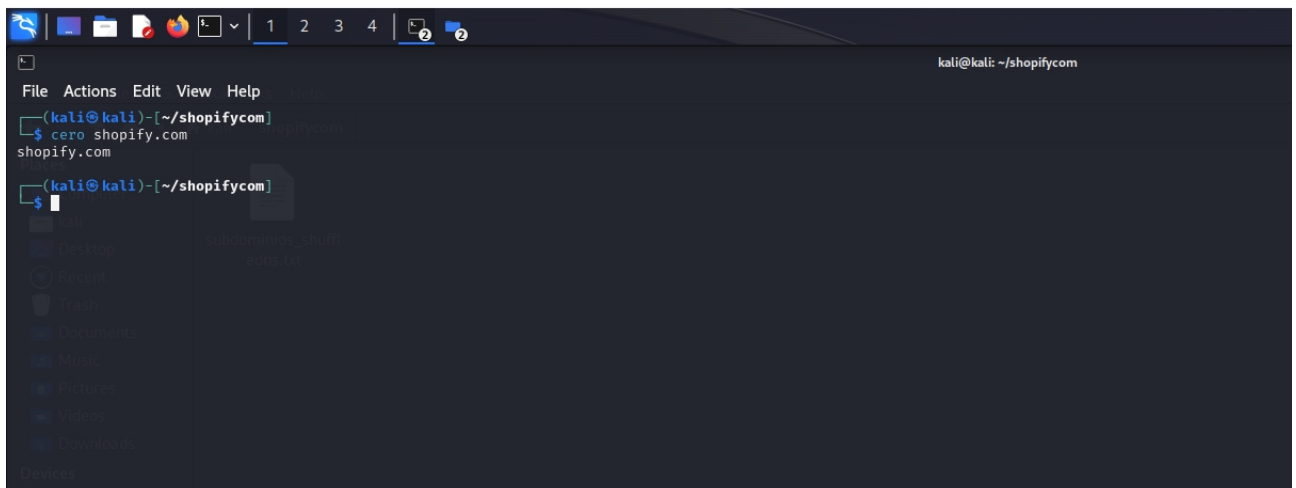
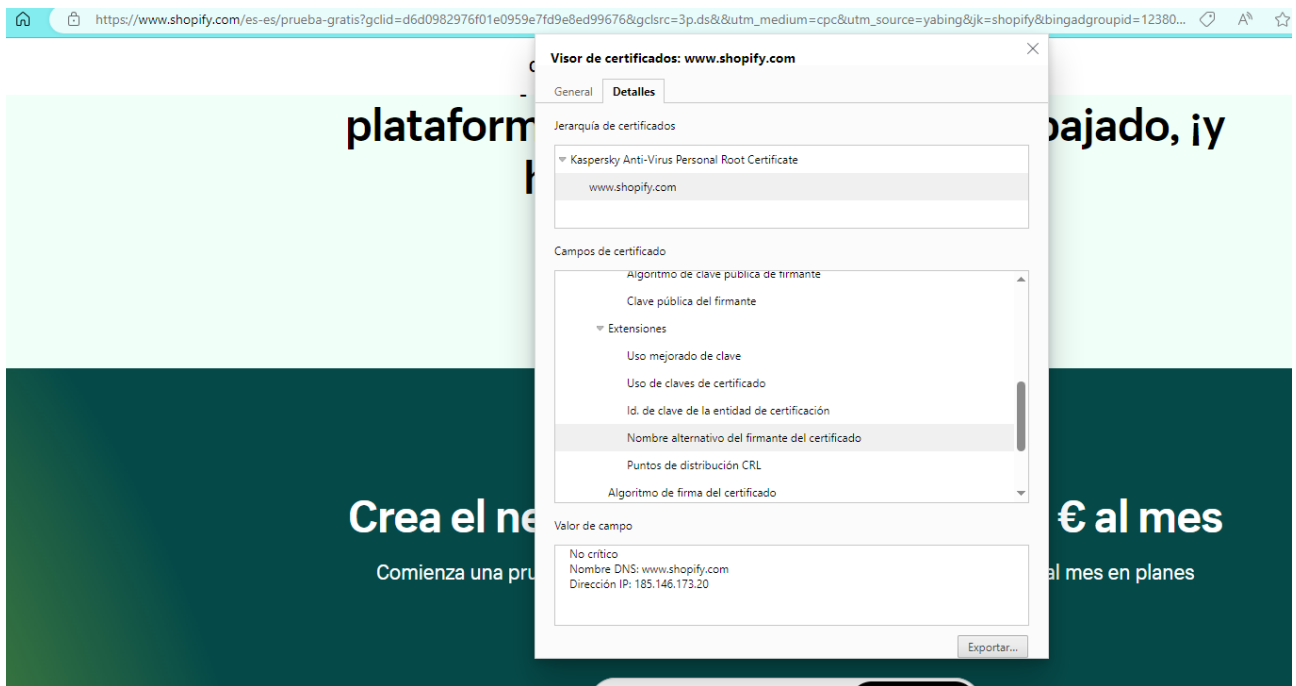
> Get related domains / subdomains by looking at Google Analytics IDs
> Python version
> By @JosueEncinar

[+] Analyzing url: https://shopify.com
[-] Tagmanager URL not found

(kali㉿kali)-[~/shopifycom]
$
```

## TLS/ Probing

Podemos utilizar la herramienta CERO para obtener dominios, subdominios a través del certificado TLS:



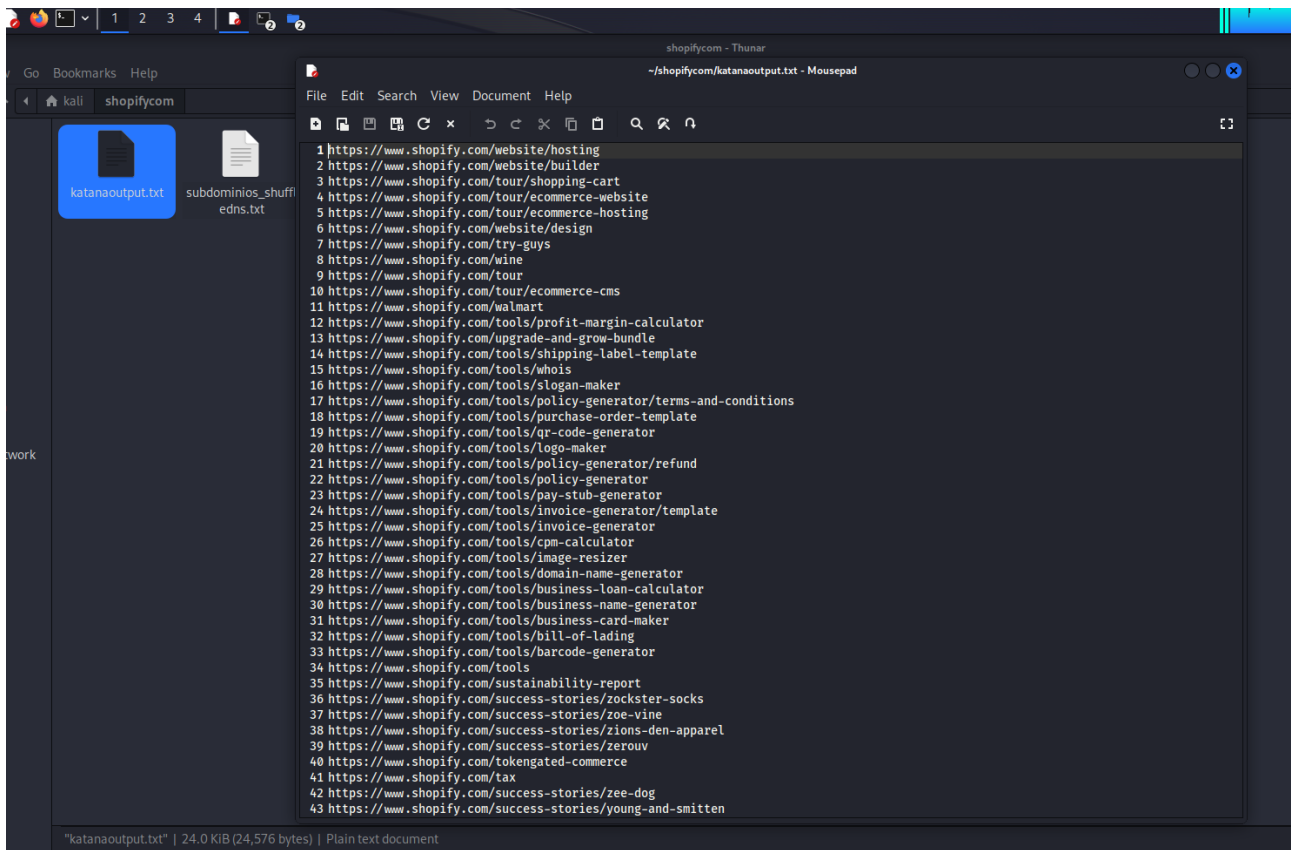
Web Scraping:

Técnica para obtener datos de las webs, podemos utilizar la herramienta KATANA:

KATANA:

echo shopify.com | katana -silent -jc -o katanaoutput.txt -kf robotstxt,sitemapxml

abrimos el fichero katanaoutput.txt y nos da estos resultados:



GAU:

gau --threads 5 shopify.com --o gauoutput.txt

abrimos el fichero gauoutput.txt

