

# Práctica 1-OSINT

Azpeitia García Karyme Ivette

Pedro Méndez Jose Manuel

## 2.1 Información personal

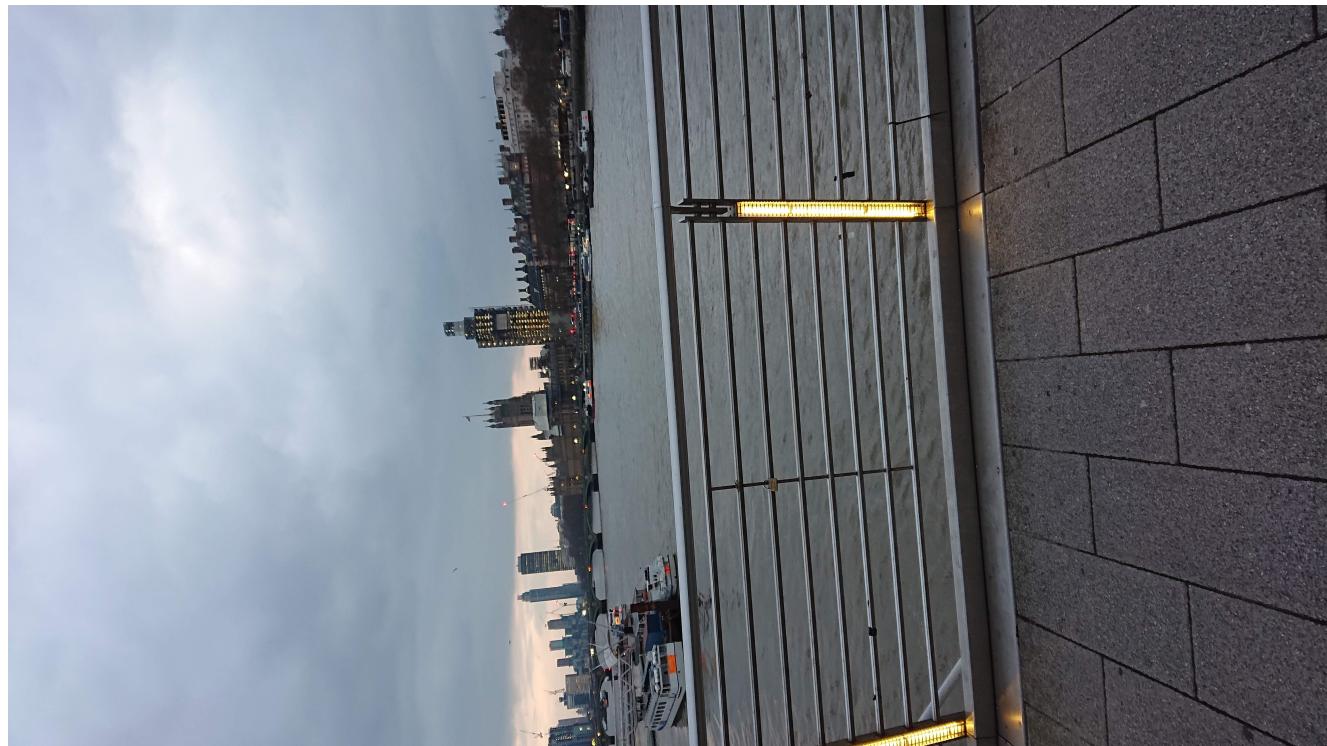


Imagen sobre la que trabajamos utilizando la herramienta: *Exif.tools*.

1. ¿Cuál es el nombre real del archivo? Es decir, el nombre que se le dió por el sistema operativo.

File name: **phpCjd4Yf**

2. ¿Qué marca es la cámara con la que fue tomada la foto?

Make: Sony  
Camera Model Name: H8216

De acuerdo a la información anterior la foto fue tomada por un celular **Sony Xperia XZ2 (H8216)**

3. ¿De qué color son las carpas del restaurante latino a unas calles?

El restaurante latino ubicado a unas calles de nombre **Las Iguanas – London – Royal Festival Hall** tiene carpas color azul cielo y rojas.

## 2.2 Información técnica de un sistema

Sitio web investigado: [Game's website](https://www.friv.com).

Para conseguir información de la pagina web será necesario conocer la dirección IP de esta.

### Obteniendo la dirección IP del website

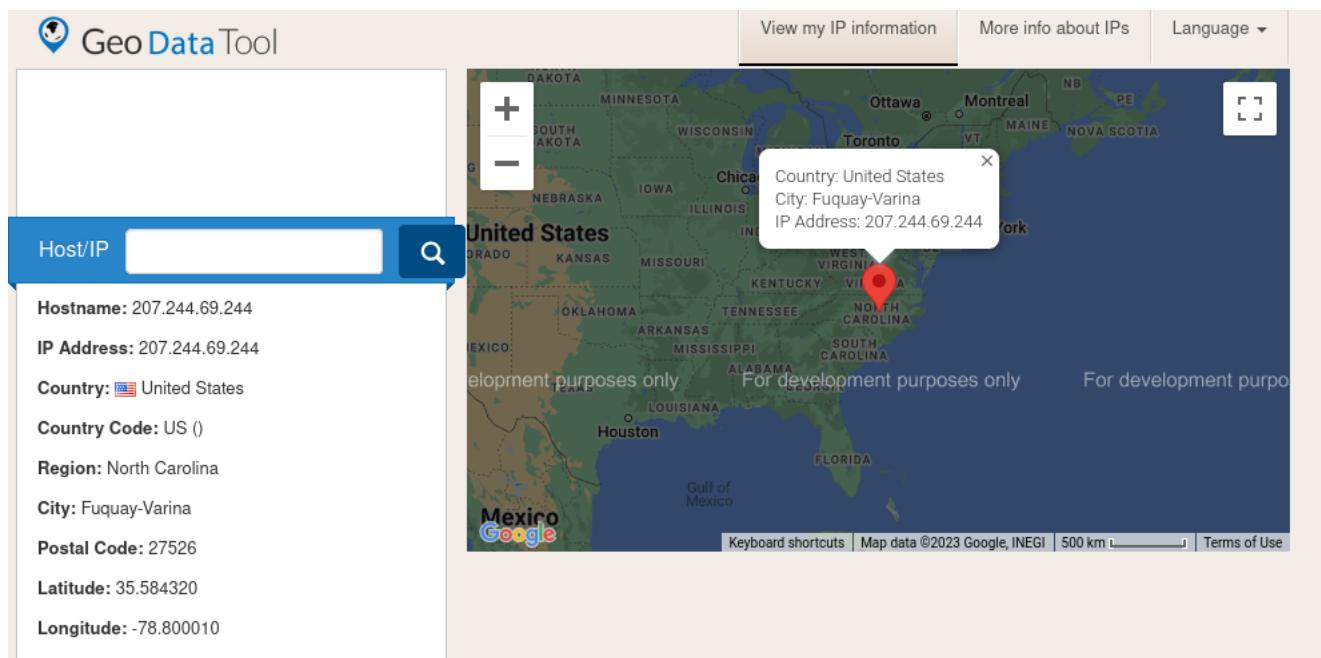
```
~ % nslookup https://www.friv.com
```

Server: 10.0.2.3  
Address: 10.0.2.3#53

Non-authoritative answer:  
Name: https://www.friv.com  
Address: 207.244.69.244

Utilizando los siguientes sitios, recabamos la siguiente información:

- [Whois.domaintools](https://whois.domaintools.com/): La localización de la dirección IP del servidor: United States Washington Mass Division Of Employment Training, pero no encontramos mucha información relevante.
- [Geo Data Tool](https://geodatatool.com/)



Información obtenida usando Geo Data Tool.

- [Who.is](https://www.whois.com/whois/www.friv.com): Aquí pudimos encontrar varias direcciones ip y saber que están trabajando con google. En este caso decidimos investigar más con:

[www.friv.com](https://www.friv.com) - A - 498 - 207.244.86.26

### Información obtenida

Hostname: 207.244.69.244  
IP Address: 207.244.69.244

#### Registrant Contact Information:

NameRedacted for Privacy  
OrganizationPrivacy service provided by Withheld for Privacy ehf  
Country: United States  
Country Code: US ()  
Region: North Carolina  
City: Fuquay-Varina  
Postal Code: 27526  
Latitude: 35.584320  
Longitude: -78.800010  
AddressKalkofnsvegur 2  
CityReykjavik  
State / ProvinceCapital Region  
Postal Code101  
CountryIS  
Phone+354.4212434

#### Administrative Contact Information:

NameRedacted for Privacy  
OrganizationPrivacy service provided by Withheld for Privacy ehf  
AddressKalkofnsvegur 2  
CityReykjavik  
State / ProvinceCapital Region  
Postal Code101  
CountryIS  
Phone+354.4212434

#### Technical Contact Information:

NameRedacted for Privacy  
OrganizationPrivacy service provided by Withheld for Privacy ehf  
AddressKalkofnsvegur 2  
CityReykjavik  
State / ProvinceCapital Region  
Postal Code101  
CountryIS  
Phone+354.4212434

- Utilizando [el motor de búsqueda de los hackers](#) nos encontramos que el SO ocupado es Debian y al momento de realizar la búsqueda nos encontramos con los puertos 22,80 y 443 abiertos.

## 2.3 Información práctica de un sistema

- Verificamos la conexión:

```
ntory@debian11:~$ ssh user@ec2-44-195-59-220.compute-1.amazonaws.com
The authenticity of host 'ec2-44-195-59-220.compute-1.amazonaws.com (44.195.59.20)' can't be established.
ECDSA key fingerprint is SHA256:dHCTNdGluQw0HalDf6AaDKYa69Bl1QqxTivt/NpNo4w.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Host key verification failed.
ntory@debian11:~$
```

---

Verificación de que la instancia está a nuestro alcance.

### 2.3.1 Escaneo de puertos usan nmap

```
ntory@debian11:~/Downloads$ nmap -V
Nmap version 7.80 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.3 openssl-1.1.1j libssh2-1.9.0 libz-1.2.11 libpcre-8.3
9 libpcap-1.10.0 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
ntory@debian11:~/Downloads$ nmap --version
Nmap version 7.80 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.3 openssl-1.1.1j libssh2-1.9.0 libz-1.2.11 libpcre-8.3
9 libpcap-1.10.0 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

---

Versión de nmap utilizada para la practica.

```
ntory@debian11:~/Downloads$ nmap ec2-44-195-59-220.compute-1.amazonaws.com -sV -Pn -sT
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-22 17:17 CST
Nmap scan report for ec2-44-195-59-220.compute-1.amazonaws.com (44.195.59.220)
Host is up (0.066s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
80/tcp    open  http     SimpleHTTPServer 0.6 (Python 3.9.2)
443/tcp   closed https
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 20.13 seconds
```

---

Resultado de la ejecución.

1. ¿Cuántos activos tiene la instancia? 3
2. ¿Cuántos puertos están cerrados? 1, el 443
3. ¿Cuántos puertos están abiertos? 2, el 22 y 80 que no esta cerrado porque es el encargado de dar el servicio.
4. ¿Cuál es la versión del puerto 80? Server: SimpleHTTP/0.6 Python 3.9.2, información obtenida con shodan
5. ¿Qué hacen los parámetros que se le pasaron a nmap?

- -sV: Nos proporciona los servicios y versiones de los puertos encontrados.
  - -Pn: Trata a los hosts como si fuera online.(skip host discovery)
  - -sT: Hace análisis de TCP SYN/Connect()/ACK/Window/Maimon
  - El aumento **-p -10000** en nmap nos permite escanear los primeros 10000 puertos.

6. Obten una lista de palabras (mejor conocida como wordlist) de algún sitio o fuente confiable, con ella realiza un escaneo y encuentra la bandera oculta dentro de la aplicación HTTP en la práctica.

Utilizando Gobuster v2.0.1 para realizar el escaneo de directorios obtuvimos:

No pude realizar la conexión.

```
ntory@debian11:~$ gobuster dir -e -u https://44.195.59.220/ -w /home/ntory/Downloads/wordlist.txt
2023/02/22 23:48:06 [!] 2 errors occurred:
  * WordList (-w): Must be specified (use `-w -` for stdin)
  * Url/Domain (-u): Must be specified

ntory@debian11:~$ gobuster dir -u https://44.195.59.220/ -w /home/ntory/Downloads/wordlist.txt
2023/02/22 23:51:16 [!] 2 errors occurred:
  * WordList (-w): Must be specified (use `-w -` for stdin)
  * Url/Domain (-u): Must be specified

ntory@debian11:~$ gobuster dir -w https://44.195.59.220/ -w /home/ntory/Downloads/wordlist.txt
2023/02/22 23:51:25 [!] 2 errors occurred:
  * WordList (-w): Must be specified (use `-w -` for stdin)
  * Url/Domain (-u): Must be specified
```

Supongo que estaba metiendo mal el servidor, porque cambiando la dirección a la proporcionada, funciono.

```
2023/02/23 00:09:07 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com/realizaba": dial tcp 44.195.59.220:80: connect: no route to host
2023/02/23 00:09:08 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com/realizamos": dial tcp 44.195.59.220:80: connect: no route to host
2023/02/23 00:09:09 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com/realista": dial tcp 44.195.59.220:80: connect: no route to host
2023/02/23 00:09:10 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com/realizando": dial tcp 44.195.59.220:80: connect: no route to host
2023/02/23 00:09:11 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com/realizan": dial tcp 44.195.59.220:80: connect: no route to host
2023/02/23 00:09:12 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com/realizara": dial tcp 44.195.59.220:80: connect: no route to host
[http://ec2-44-195-59-220.compute-1.amazonaws.com/reservacion (Status: 301)]
2023/02/23 00:09:32 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com/residentes": dial tcp 44.195.59.220:80: connect: no route to host
```

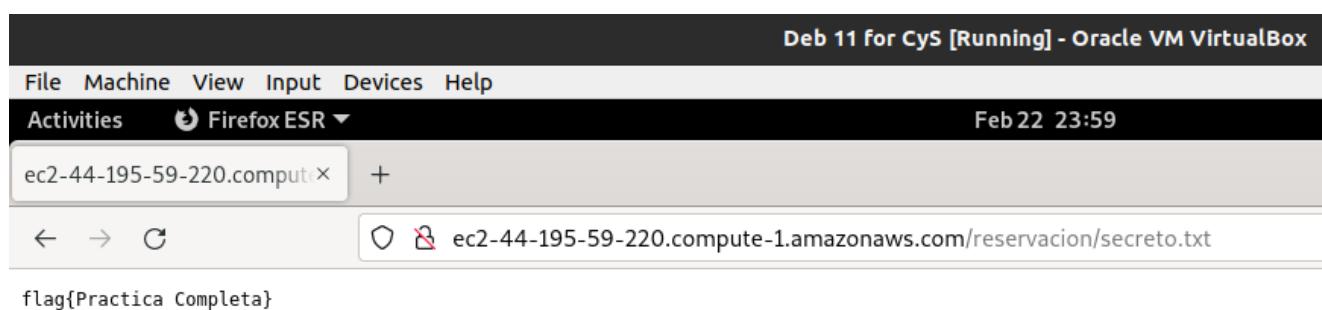
```
2023/02/23 00:09:07 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com/realizaba": dial tcp 44.195.59.220:80: connect: no route to host
2023/02/23 00:09:08 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com/realizamos": dial tcp 44.195.59.220:80: connect: no route to host
2023/02/23 00:09:09 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com/realista": dial tcp 44.195.59.220:80: connect: no route to host
2023/02/23 00:09:10 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com/realizando": dial tcp 44.195.59.220:80: connect: no route to host
2023/02/23 00:09:11 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com/realizan": dial tcp 44.195.59.220:80: connect: no route to host
2023/02/23 00:09:12 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com/realizara": dial tcp 44.195.59.220:80: connect: no route to host
http://ec2-44-195-59-220.compute-1.amazonaws.com/reservacion (Status: 301)
2023/02/23 00:09:32 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com/residentes": dial tcp 44.195.59.220:80: connect: no route to host
```

Salida con tras ejecutar: gobuster -e -u ec2-44-195-59-220.compute-1.amazonaws.com -w /home/ntory/Downloads/wordlist.txt

```
http://ec2-44-195-59-220.compute-1.amazonaws.com/usuarios (Status: 301)
http://ec2-44-195-59-220.compute-1.amazonaws.com/view (Status: 301)
2023/02/23 00:11:49 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com,
2023/02/23 00:11:49 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com,
2023/02/23 00:11:50 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com,
2023/02/23 00:11:51 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com,
2023/02/23 00:11:52 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com,
2023/02/23 00:11:53 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com,
2023/02/23 00:11:54 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com,
2023/02/23 00:11:55 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com,
2023/02/23 00:11:56 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com,
2023/02/23 00:11:57 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com,
2023/02/23 00:11:59 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com,
2023/02/23 00:11:59 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com,
headers)
2023/02/23 00:11:59 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com,
g headers)
2023/02/23 00:11:59 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com,
headers)
2023/02/23 00:11:59 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com,
ting headers)
2023/02/23 00:11:59 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com,
ting headers)
2023/02/23 00:11:59 [!] Get "http://ec2-44-195-59-220.compute-1.amazonaws.com,
ed while awaiting headers)
```

---

Salida con tras ejecutar: gobuster -e -u ec2-44-195-59-220.compute-1.amazonaws.com -w /home/ntory/Downloads/wordlist.txt



Bandera encontrada tras añadir la etiqueta de cada uno de los directorios!!!.

# Directory listing for /

---

- [aplicacion/](#)
  - [database/](#)
  - [db/](#)
  - [dbms/](#)
  - [delete/](#)
  - [get/](#)
  - [microservice/](#)
  - [post/](#)
  - [profile/](#)
  - [put/](#)
  - [reservacion/](#)
  - [table/](#)
  - [user/](#)
  - [usuarios/](#)
  - [view/](#)
- 

(aunque tambien explorando el sitio pudimos encontrar directorios valiosos).

## Notes:

---

- El aumento -p -10000 en nmap nos permite escanear los primeros 10000 puertos.
- 

📢 🎉 with ❤️ by Jose-MPM 😊 🎉 and Kary-GOD 😊 🎉 🎁