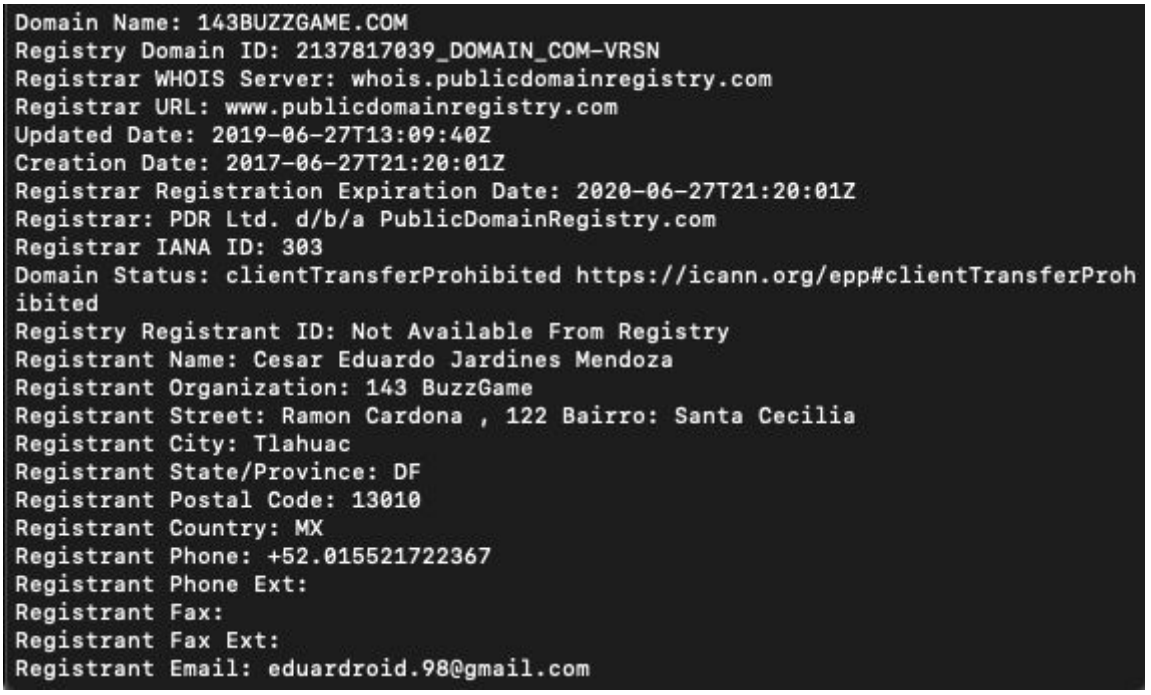
Sánchez de la Rosa César Gustavo
Jardines Mendoza César Eduardo
Emiliano Galeana Araujo
Reporte Criptografía

whois: es un protocolo de consulta y respuesta que se usa ampliamente para consultar bases de datos que almacenan a los usuarios registrados o asignados de un recurso de Internet, como un nombre de dominio, un bloque de dirección IP o un sistema autónomo , pero también se utiliza para una gama más amplia de otra información. Basta con poner en nuestra terminal whois y el dominio de la página.



nslookup: Nslookup es un programa utilizado para saber si el DNS está resolviendo correctamente los nombres y las IPs. Se utiliza con el comando nslookup, que funciona tanto en Windows como en UNIX para obtener la dirección IP conociendo el nombre, y viceversa. Basta con poner en la terminal nslookup y el dominio de la página para que nos muestre lo que queremos

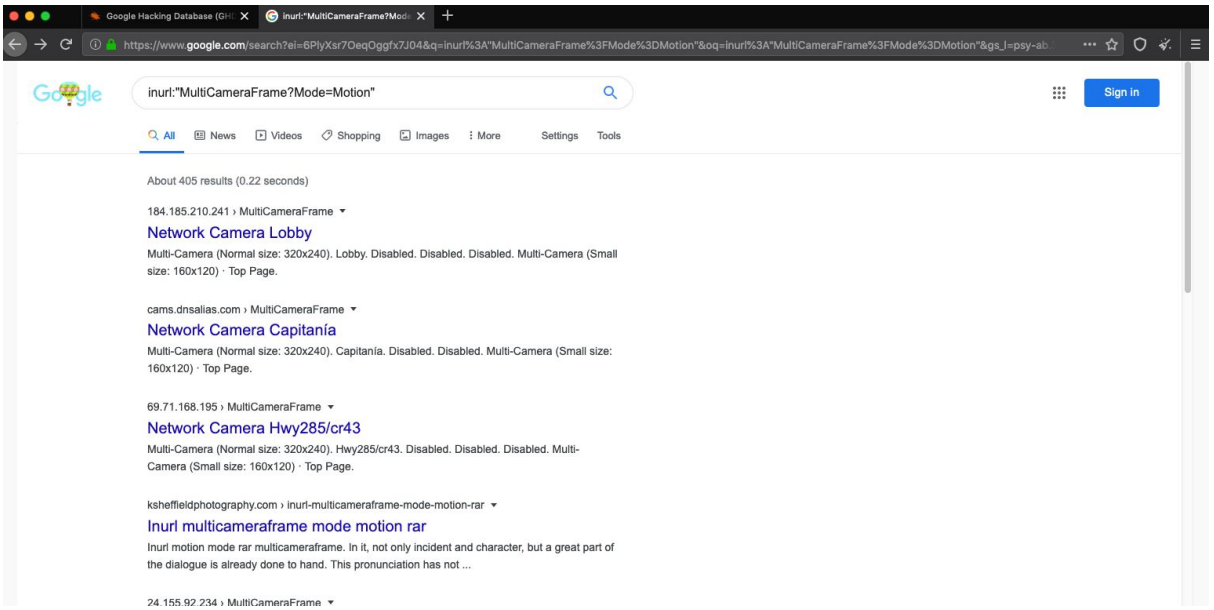
```
[MacBook-Air-de-Cesar:~ cesarjardines$ nslookup 143buzzgame.com
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
Name:   143buzzgame.com
Address: 108.179.192.149
```

Traceroute: son comandos de diagnóstico de la red para mostrar la ruta y medir los retrasos de tránsito de los paquetes a través de una red de Protocolo de Internet (IP). El historial de la ruta se registra como los tiempos de ida y vuelta de los paquetes recibidos de cada host sucesivo en la ruta; La suma de los tiempos medios en cada salto es una medida del tiempo total empleado para establecer la conexión.

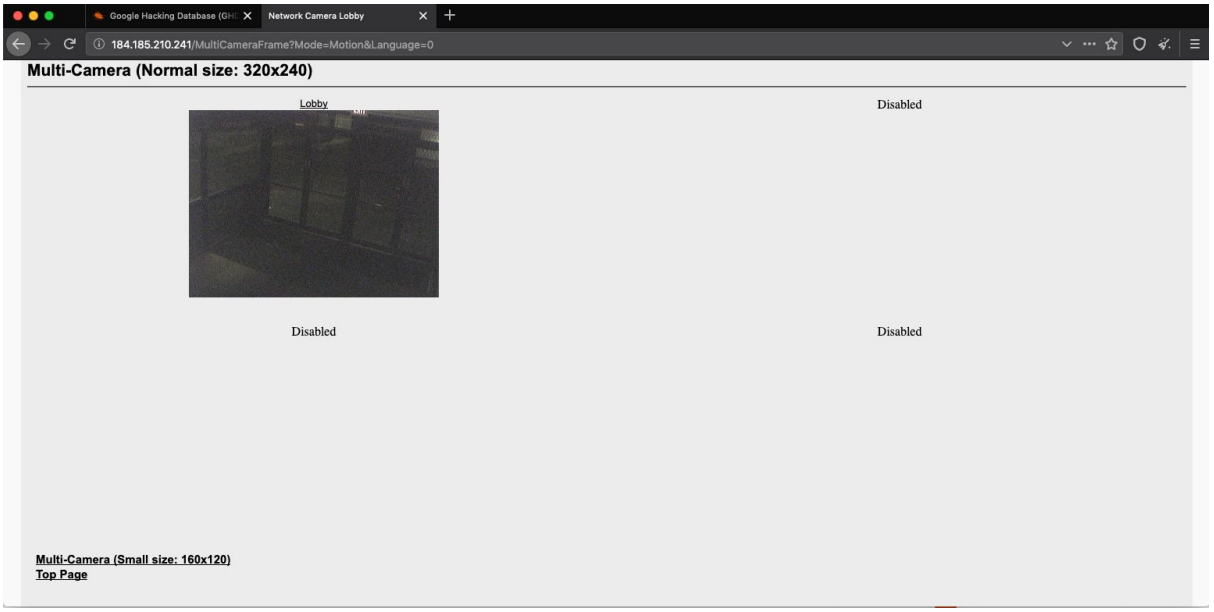
```
[MacBook-Air-de-Cesar:Downloads cesarjardines$ traceroute gmail.com
traceroute to gmail.com (172.217.15.5), 64 hops max, 52 byte packets
 1  192.168.1.254 (192.168.1.254)  2.351 ms  1.637 ms  1.947 ms
 2  ipdsl-mex-tlahuac-4-l0.uninet.net.mx (189.246.164.3)  18.016 ms  25.957 m
s  39.717 ms
 3  reg-qro-triara-27-hge0-5-0-2.uninet.net.mx (201.125.120.45)  23.627 ms  2
9.538 ms  24.809 ms
 4  74.125.50.242 (74.125.50.242)  25.505 ms  29.473 ms  24.324 ms
 5  * * *
 6  74.125.243.33 (74.125.243.33)  23.114 ms
    209.85.252.36 (209.85.252.36)  62.575 ms
    74.125.243.33 (74.125.243.33)  45.134 ms
 7  74.125.243.50 (74.125.243.50)  32.550 ms
    209.85.244.137 (209.85.244.137)  28.410 ms
    74.125.243.51 (74.125.243.51)  22.589 ms
 8  108.170.254.1 (108.170.254.1)  27.529 ms
    108.170.254.17 (108.170.254.17)  92.876 ms  50.693 ms
 9  qro01s18-in-f5.1e100.net (172.217.15.5)  21.629 ms
    209.85.243.15 (209.85.243.15)  22.533 ms
    qro01s18-in-f5.1e100.net (172.217.15.5)  25.152 ms
MacBook-Air-de-Cesar:Downloads cesarjardines$
```

Google hacking: es una herramienta para uso de información que a cierto punto puede ser delicada, cuenta con varios sitios web que cuentan con IP’s públicas y esto hace “accesible” la información. Por seguridad no descargaré nada de alguna base de datos que queramos ver.

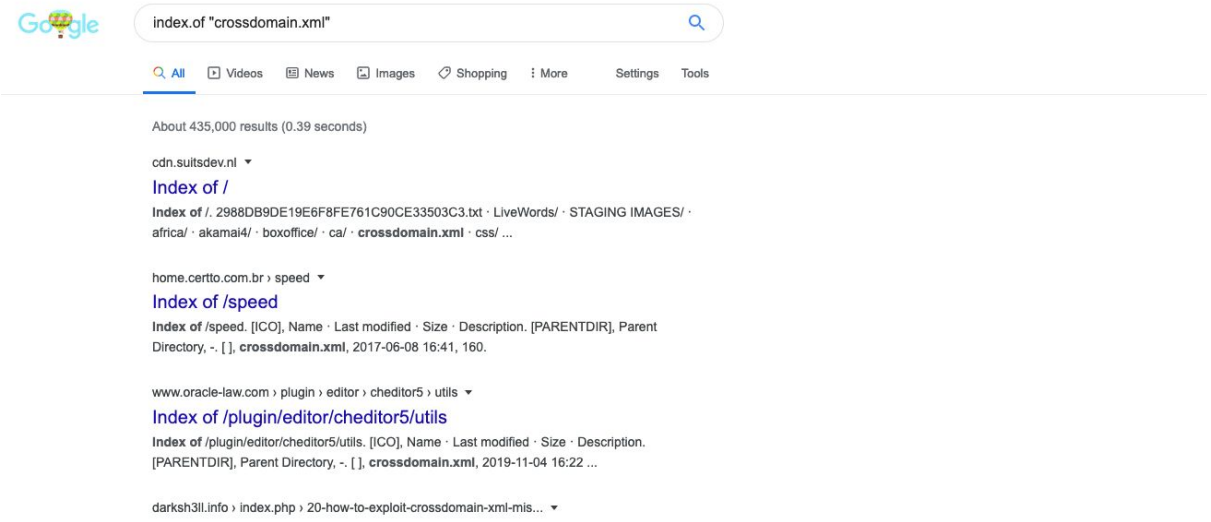
Buscamos alguna página visible que muestre sus camaras



accedemos a ella y podemos ver en tiempo lo que se transmite, estas cámaras con algunas que el portal Shodan nos muestró.



así como buscamos una cámara podemos buscar alguna base de datos, en este caso la buscamos en extensión xml.



lo cual nos da la base de datos pero como mencione no planeo abrir algo por si las dudas, pero nos podemos dar cuenta que tienen archivos xml y sabemos que puede haber información dentro.

Index of /files/Sysprep

Name	Last modified	Size	Description
Parent Directory		-	
Comando.txt	2017-10-20 11:12	107	
sysprep-uds.reg	2017-10-20 11:39	468	
unattend.xml	2017-10-23 15:53	2.2K	
Sysprep.zip	2019-11-14 14:51	1.2K	

Apache/2.4.25 (Debian) Server at images.udsenterprise.com Port 80