

# **INFORME RECOPILACIÓN DE INFORMACIÓN: INSTACART**

**ALEXANDRA OANE**

# ÍNDICE

TÉCNICAS FOOTPRINTING.....	3
TÉCNICAS FINGERPRINTING.....	15
TÉCNICAS OSINT.....	23

La empresa escogida es “Instacart.com”. Es una empresa que se dedica a la entrega de compra de alimentos a domicilio. Trabaja con varios supermercados y los usuarios pueden realizar sus compras a través de su aplicación.

Se realizarán los tres tipos de técnicas, el reconocimiento de la empresa será vertical y pasivo, en algunos puntos se emplearán también activas.

## TÉCNICAS DE FOOTPRINTIG

Se va a realizar la enumeración de diferentes máquinas, sistemas o dispositivos que pertenecen al objetivo escogido.

Al realizar la búsqueda en la página web de hackerone.com el alcance que nos muestra es el siguiente:

### **In Scope**

api.instacart.com  
www.instacart.com  
admin.instacart.com  
shoppers.instacart.com  
\*.instacart.com  
\*.instacart.tools

### **Out of Scope**

brand.instacart.com  
careers.instacart.com  
carrotstore.instacart.com  
corporate.instacart.com  
covidresponse.instacart.com  
design.instacart.com  
\*.email.instacart.com  
life.instacart.com  
news.instacart.com  
tech.instacart.com

Se comienza realizando una búsqueda con “whois” para verificar otros sitios web registrados. Este comando nos muestra el resultado de “whois” para “instacar.com”.

Domain Name: instacart.com  
Registry Domain ID: 196775\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: whois.registrar.amazon.com  
Registrar URL: https://registrar.amazon.com  
Updated Date: 2020-07-01T00:55:12.246Z  
Creation Date: 1996-10-31T05:00:00Z  
Registrar Registration Expiration Date: 2029-10-30T04:00:00Z  
Registrar: Amazon Registrar, Inc.  
Registrar IANA ID: 468  
Registrar Abuse Contact Email: abuse@amazonaws.com  
Registrar Abuse Contact Phone: +1.2067406200  
Reseller:  
Domain Status: clientTransferProhibited  
<https://icann.org/epp#clientTransferProhibited>  
Domain Status: renewPeriod <https://icann.org/epp#renewPeriod>  
Registry Registrant ID:  
Registrant Name: Domain Administrator  
Registrant Organization: Maplebear Inc.  
Registrant Street: 50 Beale St Suite 600  
Registrant City: San Francisco  
Registrant State/Province: CA  
Registrant Postal Code: 94105  
Registrant Country: US  
Registrant Phone: +1.9108172278  
Registrant Phone Ext:  
Registrant Fax:  
Registrant Fax Ext:  
Registrant Email: domains-contact@instacart.com  
Registry Admin ID:  
Admin Name: Domain Administrator  
Admin Organization: Maplebear Inc.  
Admin Street: 50 Beale St Suite 600  
Admin City: San Francisco  
Admin State/Province: CA  
Admin Postal Code: 94105  
Admin Country: US  
Admin Phone: +1.9108172278  
Admin Phone Ext:  
Admin Fax:  
Admin Fax Ext:

Admin Email: domains-contact@instacart.com  
Registry Tech ID:  
Tech Name: Domain Administrator  
Tech Organization: Maplebear Inc.  
Tech Street: 50 Beale St Suite 600  
Tech City: San Francisco  
Tech State/Province: CA  
Tech Postal Code: 94105  
Tech Country: US  
Tech Phone: +1.9108172278  
Tech Phone Ext:  
Tech Fax:  
Tech Fax Ext:  
Tech Email: domains-contact@instacart.com  
Name Server: ns-132.awsdns-16.com  
Name Server: ns-1394.awsdns-46.org  
Name Server: ns-1943.awsdns-50.co.uk  
Name Server: ns-589.awsdns-09.net  
DNSSEC: unsigned

**Se lanza con “nslookup”**

```
(kali@kali)-[~/Desktop/Instacart.com]
$ nslookup instacart.com
Server:      10.0.2.3
Address:     10.0.2.3#53

Non-authoritative answer:
Name:   instacart.com
Address: 3.222.233.151
Name:   instacart.com
Address: 34.230.254.230
Name:   instacart.com
Address: 3.214.202.113
Name:   instacart.com
Address: 34.201.97.133
Name:   instacart.com
Address: 54.198.176.47
Name:   instacart.com
Address: 34.227.250.211
Name:   instacart.com
Address: 18.210.231.158
Name:   instacart.com
Address: 44.196.95.92
```

## Datos obtenidos:

Server: 10.0.2.3  
Address: 10.0.2.3#53

Non-authoritative answer:

Name: instacart.com  
Address: 52.201.17.996  
Name: instacart.com  
Address: 18.206.51.107  
Name: instacart.com  
Address: 18.208.241.4  
Name: instacart.com  
Address: 54.152.74.152  
Name: instacart.com  
Address: 3.210.244.109  
Name: instacart.com  
Address: 3.212.180.48  
Name: instacart.com  
Address: 100.25.71.223  
Name: instacart.com  
Address: 100.24.154.81

## Con la herramienta Censys


**Se comienza con la primera dirección IP: 52.201.17.996**

No se encuentran resultados.

 Hospedadores ▾



52.201.17.996

Búsqueda

Reporte

### Hospedadores

Resultados: 0 Tiempo: 0.08s

Su consulta no arrojó resultados.

#### Consejos rápidos:

- Al buscar en el `name` campo, asegúrese de que los hosts virtuales estén incluidos en los resultados.
- Intente buscar usando un par clave:valor. La página [Definiciones de datos](#) proporciona una lista de claves.
- ¿No sabes el valor? Utilice un comodín (`*`) en su lugar para devolver hosts que tengan algún valor para el campo.
- Utilice [Informes](#) para ver qué valores suelen tener un campo.
- Coloque los criterios de búsqueda dentro de la `same_service()` función si todo debe ser cierto para un solo servi
- Utilice el operador exacto `=` para restringir los resultados a coincidencias exactas.

O consulte nuestra [introducción sobre el idioma de búsqueda](#) para obtener información detallada.

Se realiza búsqueda con la siguiente dirección: 18.206.51.107

18.206.51.107

Fecha: 18 de septiembre de 2022 12:03 a. m. UTC | Más reciente

Resumen

Explorar

Historia

QUIEN ES

Datos sin procesar

Información básica

DNS inverso

ec2-18-206-51-107.compute-1.amazonaws.com

La red

AMAZON-AES (EE. UU.)

Enrutamiento

18.204.0.0/14 a través de AS14618

Protocolos

80/HTTP , 443/HTTP

80/HTTP

TCP

Observado el 18 de septiembre de 2022 a las 12:03 a. m. UTC

Software

nginx

VER TODOS LOS DATOS

VAMOS

Detalles

http://18.206.51.107

Solicitud

OBTENER /

Protocolo

HTTP/1.1

Código de estado

301

Motivo del estado

Movido permanentemente

hachis corporal

sha1:3adb1f02d5b6054de0046e367c1d687b6cdf7aff

Título HTML

301 Movido Permanentemente

Cuerpo de respuesta

EXPANDIR

443/HTTP

TCP

Observado el 18 de septiembre de 2022 a las 12:03 a. m. UTC

Software

VER TODOS LOS DATOS

VAMOS

39°02'48.8"N 77°29'25...

Ampliar el mapa



Ubicación geográfica

Ciudad

Ashburn

Estado

Virginia

País

Estados Unidos (EE. UU.)

Coordenadas

39.0469, -77.4903

Zona horaria

América/Nueva\_York

Al no poder extraer los datos de esta herramienta, adjunto capturas de pantalla.

Lo que se obtiene de esta dirección ip, es que la empresa está situada en Estados Unidos, en el estado de Virginia, con las coordenadas, el código postal, sus servidores.

Atributo	Valor	
ip	18.206.51.107	<a href="#">Q</a>
ubicación.continente	América del norte	<a href="#">Q</a>
ubicación.país	Estados Unidos	<a href="#">Q</a>
ubicación.código_país	A NOSOTROS	<a href="#">Q</a>
ubicación.ciudad	Ashburn	<a href="#">Q</a>
ubicación.código_postal	20149	<a href="#">Q</a>
ubicación.zona horaria	América/Nueva_York	<a href="#">Q</a>
ubicación.provincia	Virginia	<a href="#">Q</a>
ubicación.coordenadas.latitud	39.0469	<a href="#">Q</a>
ubicación.coordenadas.longitud	-77.4903	<a href="#">Q</a>
ubicación.país_registrado	Estados Unidos	<a href="#">Q</a>
ubicación.código_país_registrado	A NOSOTROS	<a href="#">Q</a>
ubicación.actualizada_en	2022-09-03T08:53:42.562552Z	
sistema_autónomo.asn	14618	<a href="#">Q</a>
sistema_autónomo.descripcion	AMAZON-AES	<a href="#">Q</a>
sistema_autónomo.bgp_prefix	18.204.0.0/14	<a href="#">Q</a>
sistema_autónomo.nombre	AMAZON-AES	<a href="#">Q</a>
sistema_autónomo.código_país	A NOSOTROS	<a href="#">Q</a>
sistema_autónomo.actualizado_en	2022-09-03T08:53:42.581527Z	
dns.nombres	ec2-18-206-51-107.compute-1.amazonaws.com	<a href="#">Q</a>
dns.nombres	instacart.com	<a href="#">Q</a>
dns.records.ec2-18-206-51-107.compute-1.amazonaws.com.record_type	A	
dns.records.ec2-18-206-51-107.compute-1.amazonaws.com.resolved_at	2022-09-01T13:12:27.155203787Z	
dns.records.instacart.com.record_type	A	
dns.records.ec2-18-206-51-107.compute-1.amazonaws.com.record_type	A	
dns.records.ec2-18-206-51-107.compute-1.amazonaws.com.resolved_at	2022-09-01T13:12:27.155203787Z	
dns.records.instacart.com.record_type	A	
dns.records.instacart.com.resolved_at	2022-09-17T14:14:02.557611423Z	
dns.reverse_dns.nombres	ec2-18-206-51-107.compute-1.amazonaws.com	<a href="#">Q</a>
dns.reverse_dns.resolved_at	2022-09-07T09:24:03.136358302Z	
última_actualización_a las	2022-09-18T00:03:32.879Z	

## 80/HTTP TCP

[Ver definición](#)

Atributo	Valor	
servicios.banner	HTTP/1.1 301 Movido permanentemente\r\nFecha: <CENSURADO>\r\nContent-Type: text/html\r\nContent-Longitud: 162\r\nConexión: keep-alive\r\nServidor: nginx\r\nUbicación: http://18.206.51.107/\r\n	<a href="#">Q</a>
servicios.banner_hashes	sha256:e1dde593a63151ac8343415dc5e95641ba3f3cb20d764d3aa59237b5a6eac161	<a href="#">Q</a>
servicios.banner_hex	485454502f312e3120333031204d6f766564205065726d616e656e746c790d0a446174653a20203c52454441435445443e0a436f6e74656e742d547970653a20746578742f68746d6c0d0a436f6e74656e742d4c656e6774683a203136320d0a436f6e6e656374696f6e3a206b6565702d616c6976650d0a5365727665723a206e67696e780d0a4c6f636174696f6e3a206874740733a2f2f31382e3230362e35312e3130372f0d0a	<a href="#">Q</a>
services.extended_service_name	HTTP	<a href="#">Q</a>
services.http.request.method	OBTENER	<a href="#">Q</a>
servicios.http.request.uri	http://18.206.51.107/	<a href="#">Q</a>
services.http.request.headers.User_Agent	Mozilla/5.0 (compatible; CensysInspect/1.1; +https://about.censys.io/)	
services.http.request.headers.Acceptar	*/*	
services.http.response.protocol	HTTP/1.1	<a href="#">Q</a>
services.http.response.status_code	301	<a href="#">Q</a>



services.http.response.status_reason	Movido permanentemente	<a href="#">Q</a>
servicios.http.response.headers.Content_Length	162	<a href="#">Q</a>
services.http.response.headers.Ubicación	https://18.206.51.107/	<a href="#">Q</a>
services.http.response.headers.Servidor	nginx	<a href="#">Q</a>
services.http.response.headers.Content_Type	texto/html	<a href="#">Q</a>
services.http.response.headers.Connection	mantener viva	<a href="#">Q</a>
services.http.response.headers.Date	<ELIMINADO>	<a href="#">Q</a>
servicios.http.response.html_tags	<title>301 Movido permanentemente</title>	<a href="#">Q</a>
services.http.response.body_size	162	<a href="#">Q</a>
servicios.http.response.body	<html>\r\n<head><title>301 Movido permanentemente</title></head>\r\n<body>\r\n<center><h1>301 Movido permanentemente</h1></center>\r\n<hr><center>nginx</center>\r\n</cuerpo>\r\n</html>\r\n	<a href="#">Q</a>
servicios.http.response.body_hashes	sha256:9e17cb15dd75bbb5dbb984eda674863c3b10ab72613cf8a39a00c3e11a8492a	<a href="#">Q</a>
servicios.http.response.body_hashes	sha1:3adb1f02d5b6054de0046e367c1d687b6cdf7aff	<a href="#">Q</a>
servicios.http.response.body_hash	sha1:3adb1f02d5b6054de0046e367c1d687b6cdf7aff	<a href="#">Q</a>
servicios.http.response.html_title	301 Movido Permanentemente	<a href="#">Q</a>
servicios.http.supports_http2	falso	<a href="#">Q</a>
servicios observado_en	2022-09-18T00:03:31.506062353Z	
services.perspective_id	PERSPECTIVA_TATA	<a href="#">Q</a>
servicios.puerto	80	<a href="#">Q</a>
services.service_name	HTTP	<a href="#">Q</a>
services.software.uniform_resource_identifier	cpe:2.3:a:nginx:nginx:*****	<a href="#">Q</a>
servicios.software.part	a	<a href="#">Q</a>
proveedores.de.software.de.servicios	nginx	<a href="#">Q</a>
servicios.software.producto	nginx	<a href="#">Q</a>

servicios.software.otra.familia	nginx	<a href="#">Q</a>
servicios.software.fuente	OSI_APPLICATION_LAYER	<a href="#">Q</a>
servicios.source_ip	167.94.138.47	<a href="#">Q</a>
services.transport_protocol	TCP	<a href="#">Q</a>
servicios.truncado	falso	<a href="#">Q</a>

443/HTTP TCP

Ver definición

Atributo	Valor	
servicios.banner	HTTP/1.1 422 Entidad no procesable\r\nFecha: <ELIMINADO>\r\nContent-Type: text/html; charset=utf-8\r\nContent-Length: 34323\r\nConexión: keep-alive\r\nServidor: nginx\r\nX-DNS-Prefetch-Control: off\r\nExpect-CT: max-age= 0\r\nX-Frame-Options: SAMEORIGIN\r\nX-Strict-Transport-Security: max-age=15552000; includeSubDomains\r\nX-Download-Options: noopen\r\nX-Content-Type-Options: nosniff\r\nX-Permitted-Cross-Domain-Policies: none\r\nX-XSS-Protection: 0\r\nNETag: W/"8613-MDH/2bRLaSeJzyslpwQpNa3YITA"\r\n	<a href="#">Q</a>
servicios.banner_hashes	sha256:60759ef81e43353952ade43b7b8a18f4a954a99d581d6cb2ff3acd235474342	<a href="#">Q</a>
servicios.banner_hex	485454502f312e31203432320556e70726f6365737361626c6520456e746974790d0a446174653a20203c52454441435445443e0a436f6e74656e742d547970653a20746578742f68746d6c3b20636861727365743d7574662d380d0a436f6e74656e742d4c656e6774683a2033343332330d0a436f6e6e656374696f6e3a206b6565702d616c6976650d0a53657272665723a206e67696e780d0a582d444e532d50726566657463682d436f6e74726f6c3a206f66660d0a4578706563742d43543a206d61782d6167653d300d0a582d4672616d652d4f7074696f6e733a2053414d454f524947494e0d0a5374726963742d5472616e73706f72742d53656375726974793a206d61782d6167653d31353535323030303b20696e636c756465537562446f6d61696e730d0a582d446f776e6c6f61642d4f7074696f6e733a206e6f6f70656e0d0a582d436f6e74656e742d547970652d4f7074696f6e733a206e6f736e6966660d0a582d5065726d69747465642d43726f73732d446f6d61696e2d506f6c69636965733a206e6f6e650d0a582d5853532d50726f74656374696f6e3a20300d0a455461673a20572f22383631332d4d44482f3262524c6153654a7a79736c707751704e613359495441220d0a	<a href="#">Q</a>

En todas las direcciones obtenemos los mismos datos.

Con la herramienta <https://viewdns.info/reversewhois/?q=Instacart.com> realizamos la búsqueda y obtenemos los resultados inversos de whois.

Hay 23 dominios que coincidieron con esta consulta de búsqueda.  
Estos se enumeran a continuación:

Nombre de dominio	Fecha de creación	Registrador
cuenta-instacart.com	2022-02-11	NOM-IQ LTD. DBA COM LAUDE
analiticas-instacart.com	2018-05-09	REGISTRO DE AMAZON, INC.
californiashoppers.com	2020-12-10	REGISTRO DE AMAZON, INC.
zanahoriaswagau.com	2019-10-16	REGISTRO DE AMAZON, INC.
tiendasconectadas.es	2022-08-29	NOM-IQ LTD. DBA COM LAUDE
dardesindeelcarrito.com	2020-05-07	REGISTRO DE AMAZON, INC.
instacart-employees.us	2022-06-29	NOM-IQ LTD. DBA COM LAUDE
instacart-plus.es	2022-05-03	NOM-IQ LTD. DBA COM LAUDE
instacart.com	1996-10-31	REGISTRO DE AMAZON, INC.
instacartcareer.com	2020-12-18	REGISTRO DE AMAZON, INC.
instacartcommunityaffairs.com	2020-06-09	REGISTRO DE AMAZON, INC.
instacartfulfillment.com	2022-02-09	REGISTRO DE AMAZON, INC.
instacarthealth.us	2022-08-05	NOM-IQ LTD. DBA COM LAUDE
instacarthelp.com	2020-04-15	REGISTRO DE AMAZON, INC.
instacartimpact.com	2022-03-09	REGISTRO DE AMAZON, INC.
instacartplus.com	2022-02-17	REGISTRO DE AMAZON, INC.
instacartplus.es	2022-05-03	NOM-IQ LTD. DBA COM LAUDE
instacartroot.com	2015-08-25	GANDI SAS
instacartstore.com	2020-04-15	REGISTRO DE AMAZON, INC.
lotter.ng	2017-09-05	WEB4AFRICA
pho3nlx.in	2017-04-26	GANDI SAS (R91-AFIN)
código-de-referencia-instacart.com	2021-04-20	GODADDY.COM, LLC
marcas-instacart.com	2022-03-10	NOM-IQ LTD. DBA COM LAUDE

## AMASS

Se trata de realizar el reconocimiento vertical.

```
(kali@kali)-[~/Desktop/Instacart.com]
$ amass enum -src -d instacart.com
No names were discovered

The enumeration has finished
Discoveries are being migrated into the local database
```

## AMASS PASIVO

```
(kali㉿kali)-[~/Desktop/Instacart.com]
└─$ amass enum -v -passive -d instacart.com -src -oA scan
Querying GoogleCT for instacart.com subdomains
Querying Searx for instacart.com subdomains
Querying Arquivo for instacart.com subdomains
Querying Baidu for instacart.com subdomains
Querying CertSpotter for instacart.com subdomains
Querying RapidDNS for instacart.com subdomains
Querying Ask for instacart.com subdomains
Querying HackerTarget for instacart.com subdomains
Querying Riddler for instacart.com subdomains
Querying Sublist3rAPI for instacart.com subdomains
Querying ArchiveIt for instacart.com subdomains
Querying Mnemonic for instacart.com subdomains
Querying AlienVault for instacart.com subdomains
Querying HyperStat for instacart.com subdomains
Querying ThreatMiner for instacart.com subdomains
Querying Gists for instacart.com subdomains
Querying PKey for instacart.com subdomains
Querying Wayback for instacart.com subdomains
Querying BufferOver for instacart.com subdomains
Querying Crtsh for instacart.com subdomains
Querying Maltiverse for instacart.com subdomains
Querying ThreatCrowd for instacart.com subdomains
Querying AbuseIPDB for instacart.com subdomains
Querying SonarSearch for instacart.com subdomains
Querying AnubisDB for instacart.com subdomains
Querying Brute Forcing for instacart.com subdomains
Querying Digtorus for instacart.com subdomains
Querying HAW for instacart.com subdomains
Querying Searchcode for instacart.com subdomains
Querying URLScan for instacart.com subdomains
Querying FullHunt for instacart.com subdomains
Querying Censys for instacart.com subdomains
Querying Bing for instacart.com subdomains
Querying N45HT for instacart.com subdomains
Querying UKWebArchive for instacart.com subdomains
Querying CommonCrawl for instacart.com subdomains
Querying SiteDossier for instacart.com subdomains
Querying Greynoise for instacart.com subdomains
Querying HackerOne for instacart.com subdomains
Querying IPv4Info for instacart.com subdomains
Querying DNSDumpster for instacart.com subdomains
Querying DuckDuckGo for instacart.com subdomains
Querying Robtex for instacart.com subdomains
Querying Yahoo for instacart.com subdomains
[DNS]          instacart.com

The enumeration has finished
Discoveries are being migrated into the local database
```

El subcomando enum lleva a cabo la enumeración y el mapeo de red del objetivo en cuestión, realizando un escaneo.

## SPIDERFOOT

Buscamos dns resolve, con el siguiente comando y el flag -q:

```
spiderfoot -m sfp_dnsresolve -s instacart.com -q
```

```
(kali㉿kali)-[~/Desktop/Instacart.com]
$ spiderfoot -m sfp_dnsresolve -s instacart.com -q
```

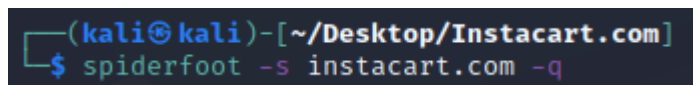
Source	Type	Data
SpiderFoot UI	Internet Name	instacart.com
SpiderFoot UI	Domain Name	instacart.com
sfp_dnsresolve	IP Address	3.222.233.151
sfp_dnsresolve	IP Address	44.206.27.163
sfp_dnsresolve	Domain Name	instacart.com
sfp_dnsresolve	IP Address	100.25.71.223
sfp_dnsresolve	IP Address	34.230.254.230
sfp_dnsresolve	IP Address	34.227.250.211
sfp_dnsresolve	IP Address	18.211.228.222
sfp_dnsresolve	IP Address	52.201.167.99
sfp_dnsresolve	IP Address	54.209.244.235
sfp_dnsresolve	Internet Name	ec2-3-222-233-151.compute-1.amazonaws.com
sfp_dnsresolve	Domain Name (Parent)	amazonaws.com
sfp_dnsresolve	Internet Name	ec2-44-206-27-163.compute-1.amazonaws.com
sfp_dnsresolve	Internet Name	ec2-100-25-71-223.compute-1.amazonaws.com
sfp_dnsresolve	Internet Name	ec2-34-230-254-230.compute-1.amazonaws.com
sfp_dnsresolve	Internet Name	ec2-34-227-250-211.compute-1.amazonaws.com
sfp_dnsresolve	Internet Name	ec2-18-211-228-222.compute-1.amazonaws.com
sfp_dnsresolve	Internet Name	ec2-52-201-167-99.compute-1.amazonaws.com
sfp_dnsresolve	Internet Name	ec2-54-209-244-235.compute-1.amazonaws.com

```
spiderfoot -m sfp_dnsbrute -s instacart.com -q
```

```
(kali㉿kali)-[~/Desktop/Instacart.com]
$ spiderfoot -m sfp_dnsbrute -s instacart.com -q
```

Source	Type	Data
SpiderFoot UI	Internet Name	instacart.com
SpiderFoot UI	Domain Name	instacart.com
sfp_dnsbrute	Internet Name	admin.instacart.com
sfp_dnsbrute	Internet Name	affiliate.instacart.com
sfp_dnsbrute	Internet Name	api.instacart.com
sfp_dnsbrute	Internet Name	atlas.instacart.com
sfp_dnsbrute	Internet Name	assets.instacart.com
sfp_dnsbrute	Internet Name	beta.instacart.com
sfp_dnsbrute	Internet Name	bugs.instacart.com
sfp_dnsbrute	Internet Name	catalog.instacart.com
sfp_dnsbrute	Internet Name	corporate.instacart.com
sfp_dnsbrute	Internet Name	cvs.instacart.com
sfp_dnsbrute	Internet Name	dc.instacart.com
sfp_dnsbrute	Internet Name	developers.instacart.com
sfp_dnsbrute	Internet Name	docs.instacart.com
sfp_dnsbrute	Internet Name	email.instacart.com
sfp_dnsbrute	Internet Name	ex.instacart.com
sfp_dnsbrute	Internet Name	incoming.instacart.com
sfp_dnsbrute	Internet Name	login.instacart.com
sfp_dnsbrute	Internet Name	news.instacart.com
sfp_dnsbrute	Internet Name	partners.instacart.com
sfp_dnsbrute	Internet Name	secure.instacart.com
sfp_dnsbrute	Internet Name	sftp.instacart.com
sfp_dnsbrute	Internet Name	www.instacart.com

Sin especificar el módulo:



Source	Type	Data
SpiderFoot UI	Internet Name	instacart.com
SpiderFoot UI	Domain Name	instacart.com
sfp_github	Public Code Repository	Name: instacart
URL: https://github.com/eitamaton/instacart		
Description: Instacart Basket Prediction		
sfp_crxcavator	Raw Data from RIRs/APIs	{ "extension_id": "mehnbp12nAiUp4NtLnoTeRlFR2diVj545pu-MbwX84XI898dprOgdGdEwKUAEvTT8Vg=w128-h128-e365-rj-sc0x00ffffff", "name": "afekaem", "icon": "https://lh3.googleusercontent.com/eEYiXiDl9ZWEDHv9G31Ba0D8ReS-DHxcAKv4iH0xGw95Dg62L2Qnacart", "platform": "Chrome", { "extension_id": "iejafkmmklidmddbenlmjiaajkkckcm", "icon": "https://lh3.XATtLOyUGTWg=w128-h128-e365-rj-sc0x00ffffff", "name": "Right Click Search for Publix on Instacart", "platform": "Chrome", { "extension_id": "nlnndpenddcilpffjldmjnadlfadcdcl", "icon": "https://ssl.gstatic.com/chrome/webstore/ima
sfp_crxcavator	Raw Data from RIRs/APIs	{ "data": { "dangerousfunction": "fpgfdmnicfolcdjopjhbcfm_1.0.0/main.js": [64] }, "extcalls": [ "https://www.amazon.com/alm/storefront?almB26linkId=9dcefe291ce664694b3fca2b441b94da8&camp=1789&creative=9325", "https://www.amazon.com/alm/storefront?almB26linkId=9dcefe291ce664694b3fca2b441b94da8&camp=1789&creative=9325" ], "manifest": { "content_scripts": [ { "matches": "http://*/*", "js": [ "https://clients2.google.com/service/update2/crx", "version": "1.0.0" ], "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaInlIns4ZFr-ez3mXEfwY6Dc7oobDEfl2K48kTY94STXLULSoI2mLosfrzq3RWiASc=w128-h128-e365-rj-sc0x00ffffff", "name": "AlPrice Search by image allows you to easily find the source goods on e-commerce websites.", "update_url": "https://clients2.google.com/service/update2/crx", "version": "1.0.0" }, "related": { "aadbaIn

Se inicia, pero tras varias horas de espera, no finaliza.

```
<div class='mb-4'>
<input name='branch quick link' type='hidden'>
<button class='text-me-submit bg-isc-green text-white block w-full p-3 mt-2 text-lg font-bold rounded-md opacity-25 cursor-not-allowed' disabled='
</div>
</form>
<div class='mb-4 flex flex-col items-center md:flex-row'>
<a href='https://instashopper.app.link/appdownload' rel='noopener noreferrer' target='_blank' title='Download Shoppers app'>

</div>
<p class='text-xs text-gray-500'>By providing my phone number above, I agree and consent to receiving messages from Instacart. Message and data rates
dialed. Message frequency varies. Text STOP to Cancel.</p>
</div>
<div>
<img loading="lazy" width="229" height="351" alt="Instacart Delivery" class="mx-auto" src="https://shoppers.instacart.com/packs/applicants/media/ap
</div>
```

```

<!-- DOWNLOAD SHOPPER APP - Need to localize app icon assets for French -->
<div class='container mx-auto px-4 mb-32'>
  <div class='grid grid-cols-1 md:grid-cols-2 gap-6'>
    <div>
      <h2 class='mb-4 text-3xl font-semibold'>Sign on, shop, and start making money</h2>
      <p>Download the Shopper App to start earning and working when you want.</p>
      <form action='/apps_send_link' class='text-me-form md:mr-16' method='post'>
        <div>
          <input autocomplete='tel' class='text-me-input border border-gray-300 p-2 block w-full mb-2' type='text'>
            <div class='text-me-error hidden text-sm text-red-500'>Please enter a valid phone number</div>
          <div class='mb-4'>
            <input name='branch_quick_link' type='hidden'>
            <button class='text-me-submit bg-isc-green text-white block w-full p-3 mt-2 text-lg font-bo

```



```

<meta content='@instacart' name='twitter:site'>
<meta content='US' name='twitter:app:country'>
<meta content='Instacart' name='twitter:app:name:iphone'>
<meta content='545599256' name='twitter:app:id:iphone'>
<meta content='Instacart' name='twitter:app:name:ipad'>
<meta content='545599256' name='twitter:app:id:ipad'>
<meta content='Instacart' name='twitter:app:name:googleplay'>
<meta content='com.instacart.client' name='twitter:app:id:googleplay'>
<link href='https://shoppers.instacart.com/assets/beetstrap/icons/Icon-76-723374c747a
<link href='https://shoppers.instacart.com/assets/beetstrap/icons/Icon-76-723374c747a
<link href='https://shoppers.instacart.com/assets/beetstrap/icons/Icon-60@2x-bbe6d64d
<link href='https://shoppers.instacart.com/assets/beetstrap/icons/Icon-76@2x-ebf9b131
<link href='https://shoppers.instacart.com/assets/beetstrap/icons/Icon-60@3x-df875578
<meta content='none' name='msapplication-config'>

```

```

8E:CF:EA:AD:5E:37:5A:24
Signature Algorithm: ecdsa-with-SHA384
Signature Value:
 30:66:02:31:00:be:59:d3:e2:dc:dc:88:2f:d9:e0:82:50:fc:
 df:e5:c3:3d:42:8c:e6:95:0a:0e:27:f5:c2:e6:f4:0f:17:cb:
 cc:c8:cd:83:d2:4c:c6:6b:9d:56:8c:90:93:de:d9:ab:ee:02:
 31:00:96:f9:52:ae:23:a0:dd:4d:a7:e4:ba:31:85:e1:6d:ea:
 f9:85:c7:bd:30:85:1c:1c:77:dc:be:1d:3e:29:f7:73:07:b7:
 dd:e2:1b:b8:e8:01:cb:53:61:18:3b:b2:93:c8

sfp_crt      Internet Name      sams-club.pbis-cf.instacart.com
sfp_crt      Internet Name      sams-club.pbis-cf.instacart.com

```

Revisando la información hasta este punto, se encuentran las imágenes de cada icono de la página web, cada uno de los distintos departamentos, los catálogos de los productos, los comentarios realizados y certificados. Hasta este punto del escaneo los datos extraídos es la inspección del front de la página web.

# TÉCNICAS FINGERPRINTING

En este punto se va a tratar de extraer información más concreta y detallada del objetivo, se comienza con un escaneo de puertos.

Escaneo de puertos:

```
(kali㉿kali)-[~/Desktop/Instacart.com]
$ nmap 18.206.51.107
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-18 11:03 EDT
Nmap scan report for ec2-18-206-51-107.compute-1.amazonaws.com (18.206.51.107)
Host is up (0.15s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 15.55 seconds
```

nmap instacart.com

Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-18 11:07 EDT

Nmap scan report for instacart.com (100.24.154.81)

Host is up (0.18s latency).

Other addresses for instacart.com (not scanned): 3.217.150.32 34.230.254.230

18.210.149.139 3.229.127.74 52.201.167.99 3.210.244.109 3.222.233.151

rDNS record for 100.24.154.81: ec2-100-24-154-81.compute-1.amazonaws.com

Not shown: 998 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Nmap nos devuelve otra dirección ip de instacart.

```
(kali㉿kali)-[~/Desktop/Instacart.com]
$ nmap 100.24.154.81
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-18 11:10 EDT
Nmap scan report for ec2-100-24-154-81.compute-1.amazonaws.com (100.24.154.81)
Host is up (0.15s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 16.08 seconds
```

Escaneo de servicios UDP:

```
(kali㉿kali)-[~/Desktop/Instacart.com]
$ sudo nmap -Pn -sUV -F -d3 instacart.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-18 10:49 EDT
Fetchfile found /usr/bin/./share/nmap/nmap-services
PORTS: Using top 100 ports found open (TCP:0, UDP:100, SCTP:0)
Fetchfile found /usr/bin/./share/nmap/nmap.xsl
The max # of sockets we are using is: 0

----- Timing report -----
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0
```

```
Read from /usr/bin/./share/nmap: nmap-payloads nmap-service-probes nmap-services.
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 539.58 seconds
Raw packets sent: 226 (13.338KB) | Rcvd: 0 (0B)
```

## ANÁLISIS WEB

Buscamos por los distintos dominios, en todos ellos obtenemos el mismo resultado.

```
(kali㉿kali)-[~/Desktop/Instacart.com]
$ wafw00f instacart.com

md5hash.txt
( woof! )
Desktop
[*] Checking https://instacart.com
[+] The site https://instacart.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2

404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway
500 Internal Error

~ WAFW00F : v2.2.0 ~
Herran The Web Application Firewall Fingerprinting Toolkit
```














## Información de dominio e IP

- IP/ASN
- Detalle de IP
- Dominios
- Árbol de dominio
- Enlaces
- Certificados



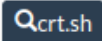
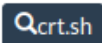
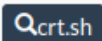
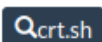
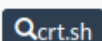
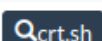
marcos

	Dirección IP	Sistema Autónomo AS
68	104.18.17.6 	13335 (NUBE FLARENET)
12	18.203.130.15 	16509 (AMAZONAS-02)
4	2a03:2880:f02d:100:cara:b00c:0:3 	32934 (FACEBOOK)
6	108.157.5.209 	16509 (AMAZONAS-02)
3	2a00:1450:4001:831::2008 	15169 (GOOGLE)
1	2a03:2880:f12d:181:cara:b00c:0:25de 	32934 (FACEBOOK)
4	34.198.65.78 	14618 (AMAZONAS-AES)
2	142.250.185.226 	15169 (GOOGLE)

## Información de dominio e IP

- IP/ASN
- Detalle de IP
- Dominios
- Árbol de dominio
- Enlaces
- Certificados

marcos

Asunto Emisor	Validez	Válido	
www.instacart.com Cloudflare Inc ECC CA-3	2022-08-16 - 2023-08-16	un año	
activos.instacart.com R3	2022-08-17 - 2022-11-15	3 meses	
*.facebook.com DigiCert SHA2 High Assurance Server CA	2022-06-28 - 2022-09-26	3 meses	
*.segment.com Amazonas	2022-01-12 - 2023-02-10	un año	
*.google-analytics.com GTS CA 1C3	2022-08-29 - 2022-11-21	3 meses	
instacart.com Amazonas	2021-10-18 - 2022-11-16	un año	
www.googleadservices.com GTS CA 1C3	2022-08-29 - 2022-11-21	3 meses	
www.bing.com Microsoft RSA TLS CA 02	2022-09-03 - 2023-03-03	6 meses	

## WHATWEB

```
(kali㉿kali)-[~/Desktop/Instacart.com]
$ whatweb www.instacart.com
http://www.instacart.com [301 Moved Permanently]
```

```
http://www.instacart.com [301 Moved Permanently] Cookies[__cf_bm,_cfuvid], C
cart.com/], UncommonHeaders[report-to,nel,x-content-type-options,cf-ray]
https://www.instacart.com/ [200 OK] Cookies[__cf_bm,_cfuvid,ahoy_track,ahoy_
ame, HTML5, HTTPServer[cloudflare], HttpOnly[__cf_bm,_cfuvid,device_uuid], I
0f1d985a581ab23358.xml], Script[application/json,application/ld+json,text/ja
from Local Stores Near You], UncommonHeaders[cf-ray,cf-cache-status,expect-c
ons[SAMEORIGIN], X-XSS-Protection[0]
```

*http://www.instacart.com [301 Moved Permanently] Cookies[\_\_cf\_bm,\_cfuvid], Country[UNITED STATES][US], HTTPServer[cloudflare], HttpOnly[\_\_cf\_bm,\_cfuvid], IP[104.18.16.6], RedirectLocation[https://www.instacart.com/], UncommonHeaders[report-to,nel,x-content-type-options,cf-ray]  
https://www.instacart.com/ [200 OK]  
Cookies[\_\_cf\_bm,\_cfuvid,ahoy\_track,ahoy\_visit,ahoy\_visitor,device\_uuid], Country[UNITED STATES][US], Email[17a73cbe32d1421bb73bc112f010623e@o502263.ingest.sentry.io], Frame, HTML5, HTTPServer[cloudflare], HttpOnly[\_\_cf\_bm,\_cfuvid,device\_uuid], IP[104.18.17.6], Object[image/svg+xml], Open-Graph-Protocol, OpenSearch[https://www.instacart.com/assets/opensearch-7a067a224705210f1d985a581ab23358.xml], Script[application/json,application/ld+json,text/javascript], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], Title[Instacart | Grocery Delivery or Pickup from Local Stores Near You], UncommonHeaders[cf-ray,cf-cache-status,expect-ct,x-content-type-options,x-dns-prefetch-control,x-download-options,x-permitted-cross-domain-policies,report-to,nel], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]*

```
[WRN] Use with caution. You are responsible for your actions.
[WRN] Developers assume no liability and are not responsible for any misuse or
damage.
[INF] nuclei-templates are not installed, installing...
[INF] Successfully downloaded nuclei-templates (v9.1.9) to
/home/kali/.local/nuclei-templates. GoodLuck!
[INF] Using Nuclei Engine 2.7.7 (latest)
[INF] Using Nuclei Templates 9.1.9 (latest)
[INF] Templates added in last update: 35
[INF] Templates loaded for scan: 3985
```

```
[INF] Templates clustered: 689 (Reduced 630 HTTP Requests)
[2022-09-18 13:29:29] [mx-fingerprint] [dns] [info] instacart.com [20
alt1.aspmx.l.google.com.,30 alt2.aspmx.l.google.com.,40
aspmx2.googlemail.com.,50 aspmx3.googlemail.com.,10 aspmx.l.google.com.]
[INF] Using Interactsh Server: oast.live
[2022-09-18 13:29:42] [nameserver-fingerprint] [dns] [info] instacart.com
[ns-1394.awsdns-46.org.,ns-589.awsdns-09.net.,ns-132.awsdns-16.com.,ns-1943.a
wsdns-50.co.uk.]
[2022-09-18 13:29:42] [caa-fingerprint] [dns] [info] instacart.com
[godaddy.com,letsencrypt.org,Digicert.com,amazon.com,comodoca.com]
```

## NIKTO

```
(kali㉿kali)-[~/Desktop/Instacart.com]
$ nikto -h https://www.instacart.com -o out.json
```

```
- Nikto v2.1.6
+ Target IP: 104.18.16.6
+ Target Hostname: www.instacart.com
+ Target Port: 443

+ SSL Info: Subject: /C=US/ST=California/L=San Francisco/O=Cloudflare,
md5hash.txt - PRA Ciphers: TLS_AES_256_GCM_SHA384
Issuer: /C=US/O=Cloudflare, Inc./CN=Cloudflare Inc ECC CA
+ Message: Multiple IP addresses found: 104.18.16.6, 104.18.17.6
+ Start Time: 2022-09-18 13:36:49 (GMT-4)

+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user
+ Uncommon header 'nel' found, with contents: {"success_fraction":0.01,"report
+ Uncommon header 'report-to' found, with contents: {"endpoints":[{"url":"http
bknRALTDd1Bsb1YrFJlf5np%2BvdcCCMplAFAZiOCabzXa5aRBfA3c"}],"group":"cf-nel","ma
+ The site uses SSL and Expect-CT header is not present.
+ All CGI directories 'found', use '-C none' to test none
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening str
s/LW2.pm line 5157.
at /var/lib/nikto/plugins/LW2.pm line 5157.
; at /var/lib/nikto/plugins/LW2.pm line 5157.
+ Scan terminated: 20 error(s) and 4 item(s) reported on remote host
+ End Time: 2022-09-18 13:47:53 (GMT-4) (664 seconds)

+ 1 host(s) tested
```

# TÉCNICAS OSINT

## INTELIGENCIA X

```
www.instacart.com - Instacart: comestibles entregados desde tiendas locales 2020-05-25 - 2020-11-04
├─ entrega de comestibles
│ └─ ca/near-me-in-los-angeles-ca - Entregas de comestibles cerca de mí en Los Angeles, CA | Instacart 2020-11-04
│ └─ fl/near-me-in-miami-fl - Entregas de comestibles cerca de mí en Miami, FL | Instacart 2020-11-04
│ └─ il/near-me-in-chicago-il - Entregas de comestibles cerca de mí en Chicago, IL | Instacart 2020-11-04
│ └─ ny/near-me-in-new-york-ny - Entregas de comestibles cerca de mí en Nueva York, NY | Instacart 2020-11-04
│ └─ tx/near-me-in-austin-tx - Entregas de comestibles cerca de mí en Austin, TX | Instacart 2020-11-04
└─ landing?
gclid=CjwKCAjw19z6BRAYEiwAmo64Lfts3H0e43avI0x4RQn_hqcT4yzXH90mV4uzRKYHAFR0uTU4bwCReBoCLHsQAvD_BwE&mrid=88720783&product_id=19548421f
8145171519_campaignid=1700095389_adgroupid=86977167996_device=c&utm_medium=sem_shopping&utm_source=instacart_google - Kite Hill Yog
├─ petco - Petco Delivery - Instacart 2020-11-04
safeway /products/18032650-curious-beasts-blood-red-wine-750-ml - Curious Beasts Blood Red Wine (750 ml) de Safeway - Instacart 20
└─ uwajimaya- Entrega Uwajimaya - Instacart 2020-11-04
```

## Búsqueda de emails

Con la herramienta web <https://hunter.io/search/instacart.com>, se buscan los emails relacionados con la empresa. Obtenemos los siguientes resultados:

Correos corporativos de los empleados de la empresa.

Executive (1)			IT / Engineering (1)			Marketing (2)			✉		
<b>Ankur Damani</b> Senior Marketing Manager											
ankur.damani@instacart.com											
<b>Laura Jones</b> Marketing Vp											
laura.jones@instacart.com											
<b>David Pal</b>											
david.pal@instacart.com											
<b>Viktor Evdokimov</b> Senior Software Engineer											
viktor@instacart.com											
<b>Mathieu Ripert</b> General Manager											
mathieu@instacart.com											
<b>Mark Schaaf</b> CTO											
schaaf@instacart.com											

<b>Talia Thomson</b> talia.thomson@instacart.com ● ✓	+ ⓘ 2 sources ▾
<b>Kelly Pakula</b> General Manager kelly.pakula@instacart.com ✓	+ ⓘ 2 sources ▾
<b>Apoorva Mehta</b> CEO apoorva@instacart.com ✓	+ ⓘ 5 sources ▾
jenn@instacart.com ✓	+ ⓘ 1 source ▾

Con la herramienta web <https://app.anymailfinder.com/search/single>, he buscado por nombre y empresa y todos los correos están verificados. Esta comprobación se ha realizado aunque ya aparezca en las capturas que los correos están verificados.

Se realiza búsqueda con Spiderfoot:


```
(kali㉿kali)-[~/Desktop/Instacart.com]
$ spiderfoot -s instacart.com -t EMAILADDR -f -x -q
```

Source	Type	Data
sfp_skymem	Email Address	happycustomers@instacart.com
sfp_skymem	Email Address	shoppers@instacart.com
sfp_skymem	Email Address	jobs@instacart.com
sfp_skymem	Email Address	doug@instacart.com
sfp_skymem	Email Address	press@instacart.com
sfp_skymem	Email Address	partners@instacart.com
sfp_skymem	Email Address	legal@instacart.com
sfp_skymem	Email Address	bd@instacart.com
sfp_skymem	Email Address	ordering@instacart.com
sfp_skymem	Email Address	online@instacart.com
sfp_skymem	Email Address	shopperssupport@instacart.com
sfp_skymem	Email Address	apoorva@instacart.com
sfp_skymem	Email Address	aditya@instacart.com
sfp_skymem	Email Address	info@instacart.com
sfp_skymem	Email Address	matt@instacart.com
sfp_skymem	Email Address	tim@instacart.com
sfp_skymem	Email Address	amy@instacart.com
sfp_skymem	Email Address	arbitration-opt-out@instacart.com
sfp_skymem	Email Address	copyright@instacart.com
sfp_skymem	Email Address	ler@instacart.com
sfp_skymem	Email Address	help@instacart.com
sfp_skymem	Email Address	cs@instacart.com
sfp_skymem	Email Address	brandon@instacart.com
sfp_skymem	Email Address	feedback@instacart.com



sfp_skymem	Email Address	derrick@instacart.com
sfp_skymem	Email Address	orders@instacart.com
sfp_skymem	Email Address	ash@instacart.com
sfp_skymem	Email Address	daniel.langston@instacart.com
sfp_skymem	Email Address	matthew@instacart.com
sfp_skymem	Email Address	david@instacart.com
sfp_skymem	Email Address	sean@instacart.com
sfp_skymem	Email Address	nick@instacart.com
sfp_skymem	Email Address	max@instacart.com
sfp_skymem	Email Address	u003chappycustomers@instacart.com
sfp_skymem	Email Address	maurice@instacart.com
sfp_skymem	Email Address	tye@instacart.com
sfp_skymem	Email Address	u003corders@instacart.com
sfp_skymem	Email Address	sid@instacart.com
sfp_skymem	Email Address	maksim@instacart.com
sfp_skymem	Email Address	csjobs@instacart.com
sfp_skymem	Email Address	fairway@instacart.com
sfp_skymem	Email Address	u003cno-reply@instacart.com
sfp_skymem	Email Address	u003eml.jobs@instacart.com
sfp_skymem	Email Address	vishwa@instacart.com
sfp_skymem	Email Address	ml.jobs@instacart.com
sfp_skymem	Email Address	jaime@instacart.com
sfp_skymem	Email Address	shoppersfood@instacart.com

Con los correos obtenidos de los trabajadores se ha realizado una búsqueda en las plataformas de LinkedIn y Facebook. Los usuarios tienen activados los perfiles privados. Sin embargo, parte de datos sobre una de las empleadas sí se han encontrado.



**kelly pakula**  
Vicepresidente, Comunicaciones Corporativas

[Instacart](#)

San Francisco, California, Estados Unidos

**Fundar4 correos electrónicos:**  
instacart.com, gmail.com, zynga.com, shiftcomm.com

**Teléfonos encontrados:**  
415-254-XXXX, 617-779-XXXX, 415-245-XXXX, 415-591-XXXX, 909-226-XXXX, 415730XXX


[+](#) ...

**Ubicación** San Francisco, California, Estados Unidos

**Trabajar** Vicepresidente, Comunicaciones Corporativas @ Instacart  
[Ver más](#)

**Educación** Ariz

**Habilidades** Microsoft Excel, Gestión, Gestión de proyectos, Periodismo, Liderazgo, Relaciones públicas, Planificación estratégica, Comunicaciones corporativas, Redacción de noticias, Reportajes de investigación, Facebook, Conciencia de marca, Blogging, Estrategia de contenidos, Comunicaciones estratégicas, Redes sociales, Comunicaciones de crisis, Comunicaciones internas, Marketing Comunicaciones, Medios Digitales, Publicidad, Redacción, Marketing Online, Marketing Integrado, Nuevos Medios



**Instacart**  
Alimentos y Bebidas, Comestibles

[Ver página de empresa](#)

- kelly pakula
- Vicepresidente, Comunicaciones Corporativas

## Instacart

San Francisco, California, Estados Unidos

### 4 correos electrónicos:

- instacart.com
- gmail.com
- zynga.com
- shiftcomm.com

### Teléfonos encontrados:

- 415-254-XXXX
- 617-779-XXXX
- 415-245-XXXX
- 415-591-XXXX
- 909-226-XXXX
- 415730XXX



- [kelly.pakula@instacart.com](mailto:kelly.pakula@instacart.com)
- [kpakula@gmail.com](mailto:kpakula@gmail.com)

En el informe realizado, se ha tratado de usar las distintas herramientas presentadas en el módulo para poder realizar un recopilación de información del objetivo elegido. Tras aplicar varios tipos de escaneos, la información que se ha extraído, en algunos puntos es escasa. El objetivo al tener otros subdominios de los distintos supermercados, sale del alcance.

Las siguientes herramientas que no han funcionado correctamente: “mapcidr”, “cero”, “crobot”, “amass”, “puredns”.