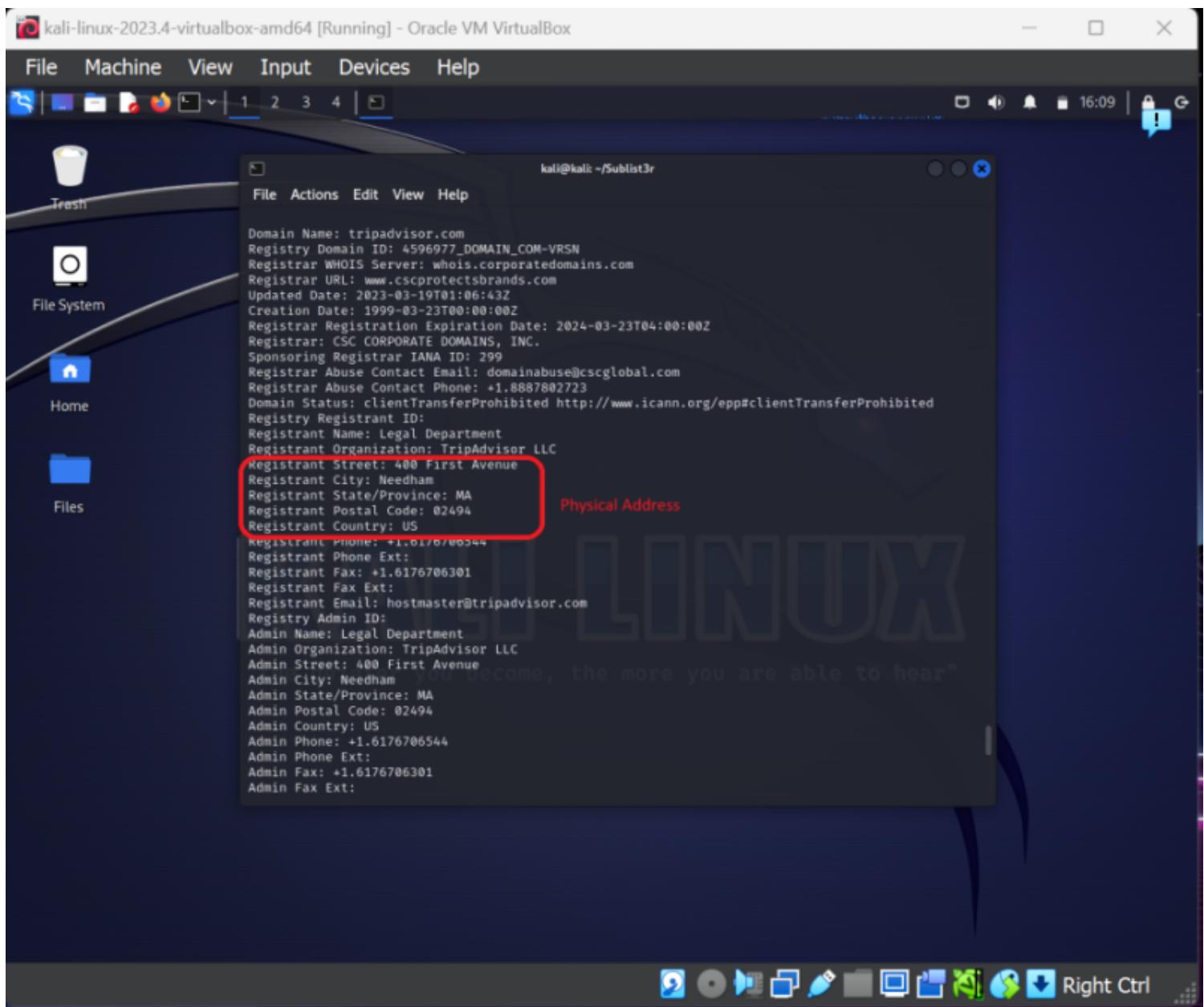


Physical Address

Mariam Khaled 7004693



```
kali@kali: ~/Sublist3r
File Actions Edit View Help
Domain Name: tripadvisor.com
Registry Domain ID: 4596977_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2023-03-19T01:06:43Z
Creation Date: 1999-03-23T00:00:00Z
Registrar Registration Expiration Date: 2024-03-23T04:00:00Z
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Legal Department
Registrant Organization: TripAdvisor LLC
Registrant Street: 400 First Avenue
Registrant City: Needham
Registrant State/Province: MA
Registrant Postal Code: 02494
Registrant Country: US
Registrant Phone: +1.6176706544
Registrant Phone Ext:
Registrant Fax: +1.6176706301
Registrant Fax Ext:
Registrant Email: hostmaster@tripadvisor.com
Registry Admin ID:
Admin Name: Legal Department
Admin Organization: TripAdvisor LLC
Admin Street: 400 First Avenue
Admin City: Needham
Admin State/Province: MA
Admin Postal Code: 02494
Admin Country: US
Admin Phone: +1.6176706544
Admin Phone Ext:
Admin Fax: +1.6176706301
Admin Fax Ext:
```

Physical Address

- 1) I used the WHOIS lookup functionality for tripadvisor.com to access and retrieve detailed information about the physical address associated with the domain registration. This information includes the precise street address, city, state, postal code, and country where the domain owner or registrant resides.

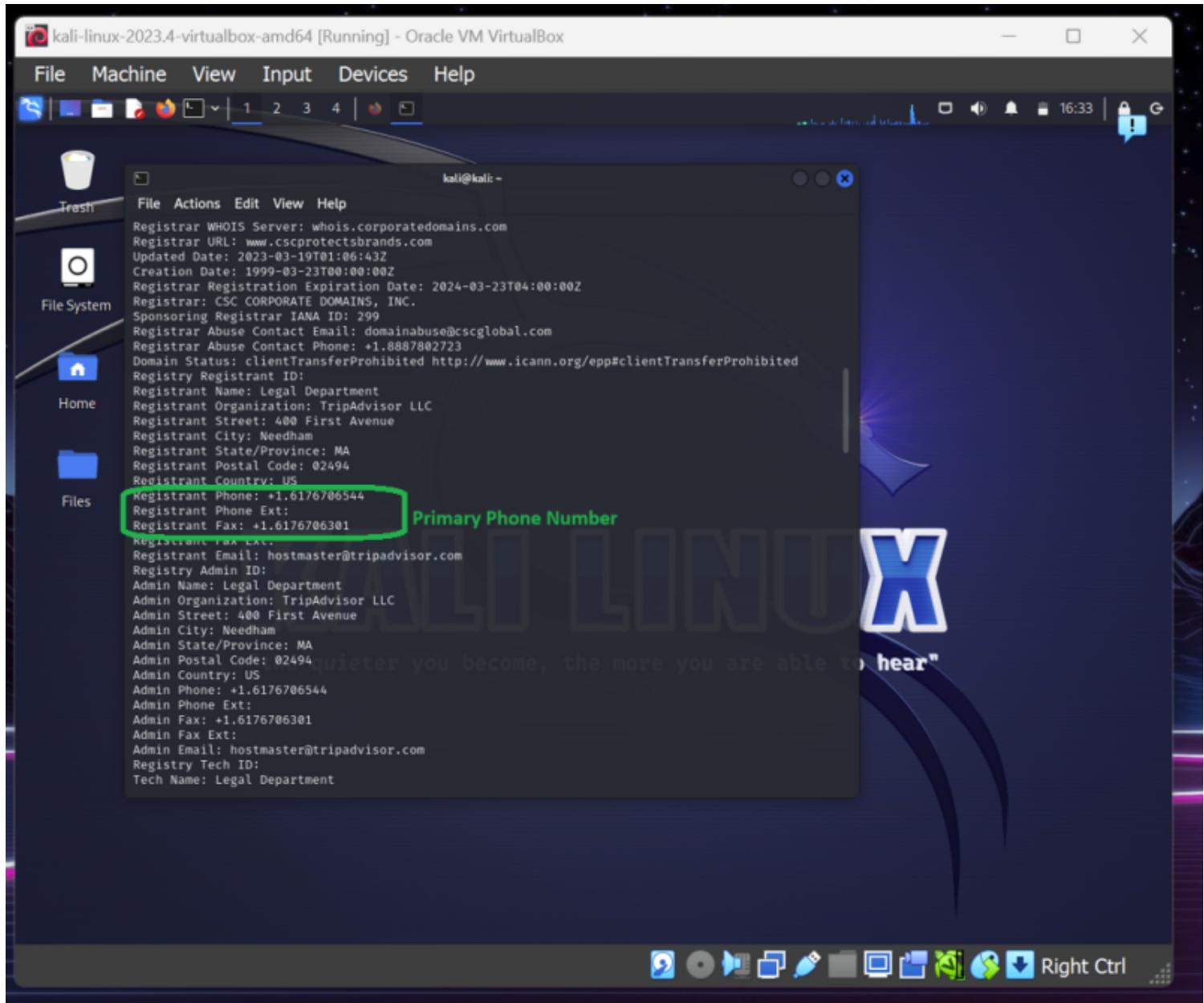
The screenshot shows a Kali Linux desktop environment with a Firefox browser window open. The browser is displaying the Tripadvisor contact page at <https://tripadvisor.mediaroom.com/US-contact-us>. The page features a green wooden barrel in a grassy field as the background image. A navigation bar at the top includes links for About Tripadvisor, Investor Relations, Resources, and Contact Us. On the left, there's a sidebar with links for Press Releases, Logo & Guidelines, Equity, Diversity + Inclusion, Social Impact, Trust & Safety, Case Studies, and Business Marketing Tools. The main content area is titled "General Contact Information" and contains a section for "Physical Address" with the address "Tripadvisor Inc., 400 1st Avenue, Needham, MA, USA 02494" and a general company phone number. Below this, there's a question about traveler help and a note about customer service questions. At the bottom, there's a section for "Data Erasure Requests" and a note about respecting user data protection rights. The desktop taskbar at the bottom shows various application icons.

2) Another way to find Tripadvisor's physical address is by visiting their website. They often provide their office location on the "Contact Us" or "About Us" page.

Phone Numbers

1) Through a WHOIS lookup for tripadvisor.com, I discovered phone numbers associated with the primary contact for domain registration and administrative purposes.

i Phone numbers for the registrant, administrative contacts, and technical contacts are among the details that WHOIS offers in relation to a domain name registration.



```
File Actions Edit View Help
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2023-03-19T01:06:43Z
Creation Date: 1999-03-23T00:00:00Z
Registrar Registration Expiration Date: 2024-03-23T04:00:00Z
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Legal Department
Registrant Organization: TripAdvisor LLC
Registrant Street: 400 First Avenue
Registrant City: Needham
Registrant State/Province: MA
Registrant Postal Code: 02494
Registrant Country: US
Registrant Phone: +1.6176706544
Registrant Phone Ext:
Registrant Fax: +1.6176706301
Registrant Fax Ext:
Registrant Email: hostmaster@tripadvisor.com
Registry Admin ID:
Admin Name: Legal Department
Admin Organization: TripAdvisor LLC
Admin Street: 400 First Avenue
Admin City: Needham
Admin State/Province: MA
Admin Postal Code: 02494
Admin Country: US
Admin Phone: +1.6176706544
Admin Phone Ext:
Admin Fax: +1.6176706301
Admin Fax Ext:
Admin Email: hostmaster@tripadvisor.com
Registry Tech ID:
Tech Name: Legal Department
```

2) During my investigation, I also discovered phone numbers linked to employee email addresses on Hunter.io.

i When Hunter.io retrieves email addresses associated with a domain, it also looks for other contact information, such as phone numbers, if available.

Phone Numbers

3) Another way to find Tripadvisor's phone numbers is by visiting their website. They often provide their office location on the "Contact Us" or "About Us" page.

United States▼

General Contact Information

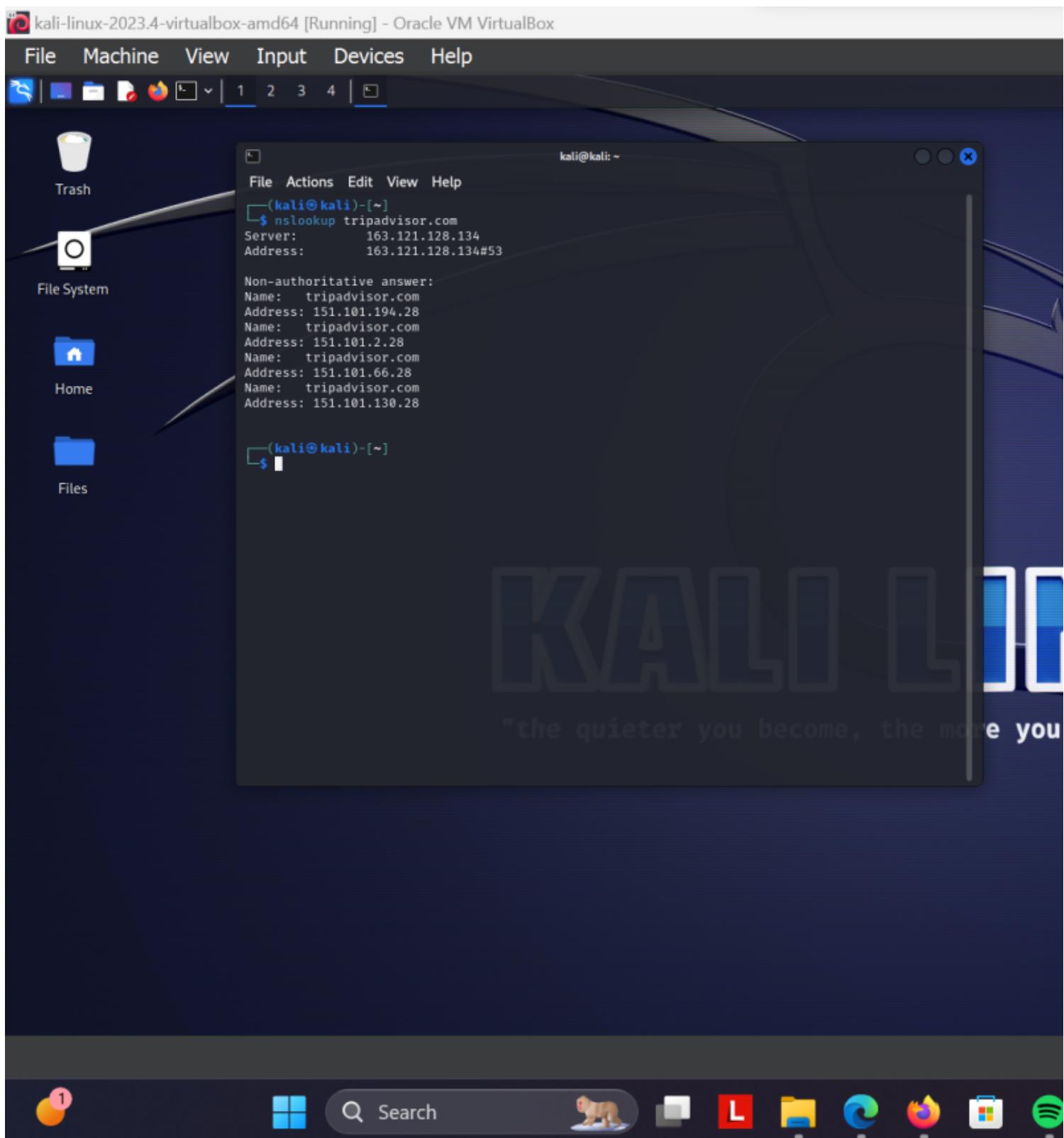
Mailing address: Tripadvisor Inc., 400 1st Avenue, Needham, MA, USA 02494
General company phone number: +1 781 800 5000 **Phone Number**

Are you a traveler in need of help? Have a question about your review? Problems booking your hotel, flight or attraction/activity? Trouble with a restaurant reservation?

We want to help! Did you know that nearly every customer service questions can be answered by visiting our easy-to-use [Help Center](#)?

Still need support? Visit our [general inquiries](#) page and someone from Tripadvisor's customer support team will respond as soon as possible!

IP Addresses



1) The nslookup command for tripadvisor.com enabled the retrieval of its associated IP addresses.

i Nslookup is a network administration tool that queries DNS (Domain Name System) servers to convert domain names into IP addresses.

The screenshot shows a Kali Linux desktop environment. A terminal window is open, displaying the output of the `dig tripadvisor.com` command. The terminal window title is `kali@kali: ~`. The output shows the following:

```
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****
[!] Invalid source.

(kali㉿kali)-[~]
$ dig tripadvisor.com

; <>> DiG 9.19.17-2~kali1-Kali <>> tripadvisor.com
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 18133
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1220
;; COOKIE: b9ac274d881e0951a589fbe265d669a5954b8b9e3faca41a (good)
;; QUESTION SECTION:
;tripadvisor.com.           IN      A

;; ANSWER SECTION:
tripadvisor.com.      37      IN      A      151.101.66.28
tripadvisor.com.      37      IN      A      151.101.130.28
tripadvisor.com.      37      IN      A      151.101.194.28
tripadvisor.com.      37      IN      A      151.101.2.28

;; Query time: 12 msec
;; SERVER: 163.121.128.134#53(163.121.128.134) (UDP)
;; WHEN: Wed Feb 21 16:22:43 EST 2024
;; MSG SIZE rcvd: 136

(kali㉿kali)-[~]
$
```

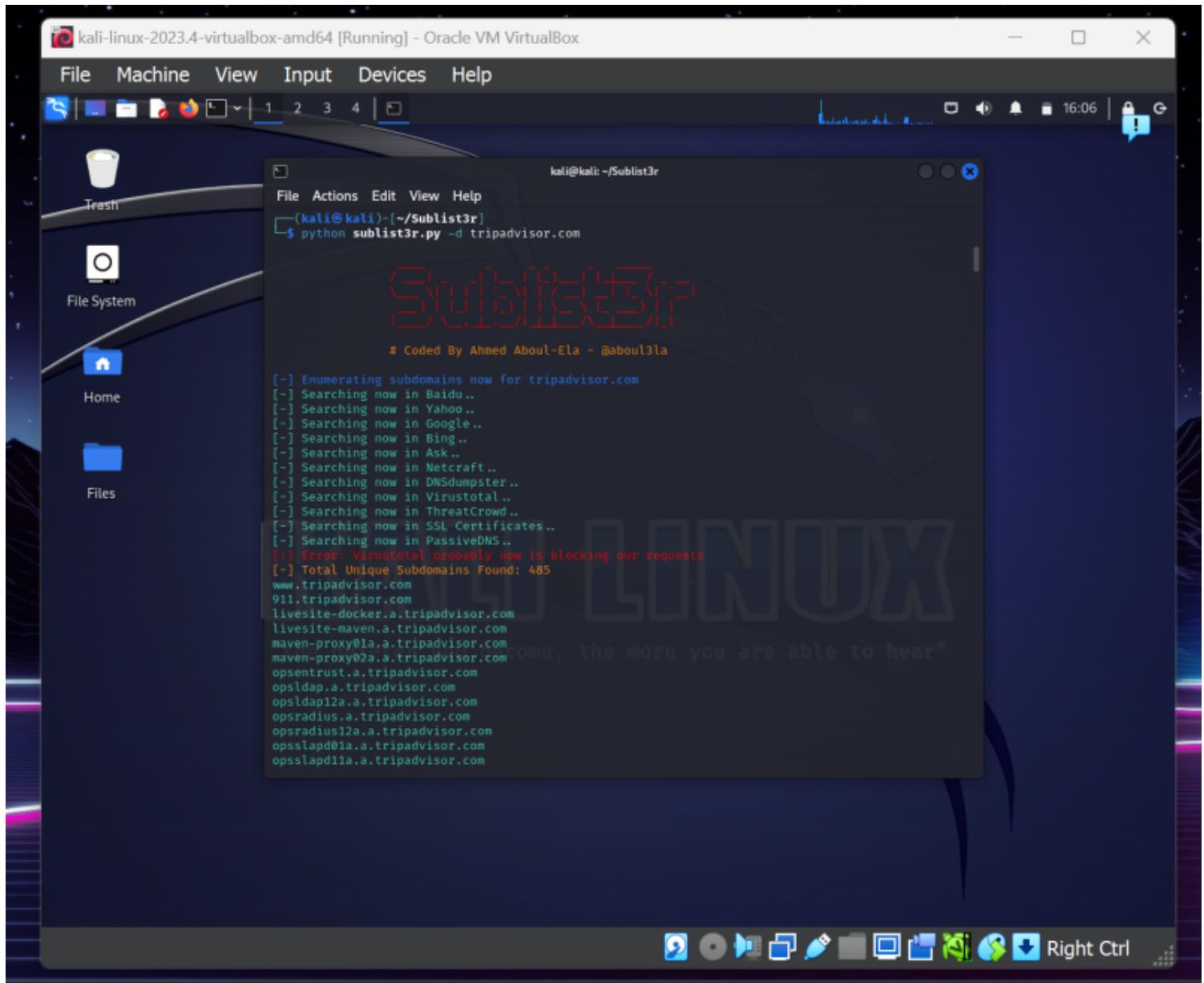
2) **Dig**, which stands for Domain Information Groper, is a network administration tool used to query DNS (Domain Name System) servers for various types of DNS records.

This process enables the translation of domain names into their corresponding IP addresses.

Subdomains

1) Sublist3r generated a list of subdomains related to the target domain "tripadvisor.com"

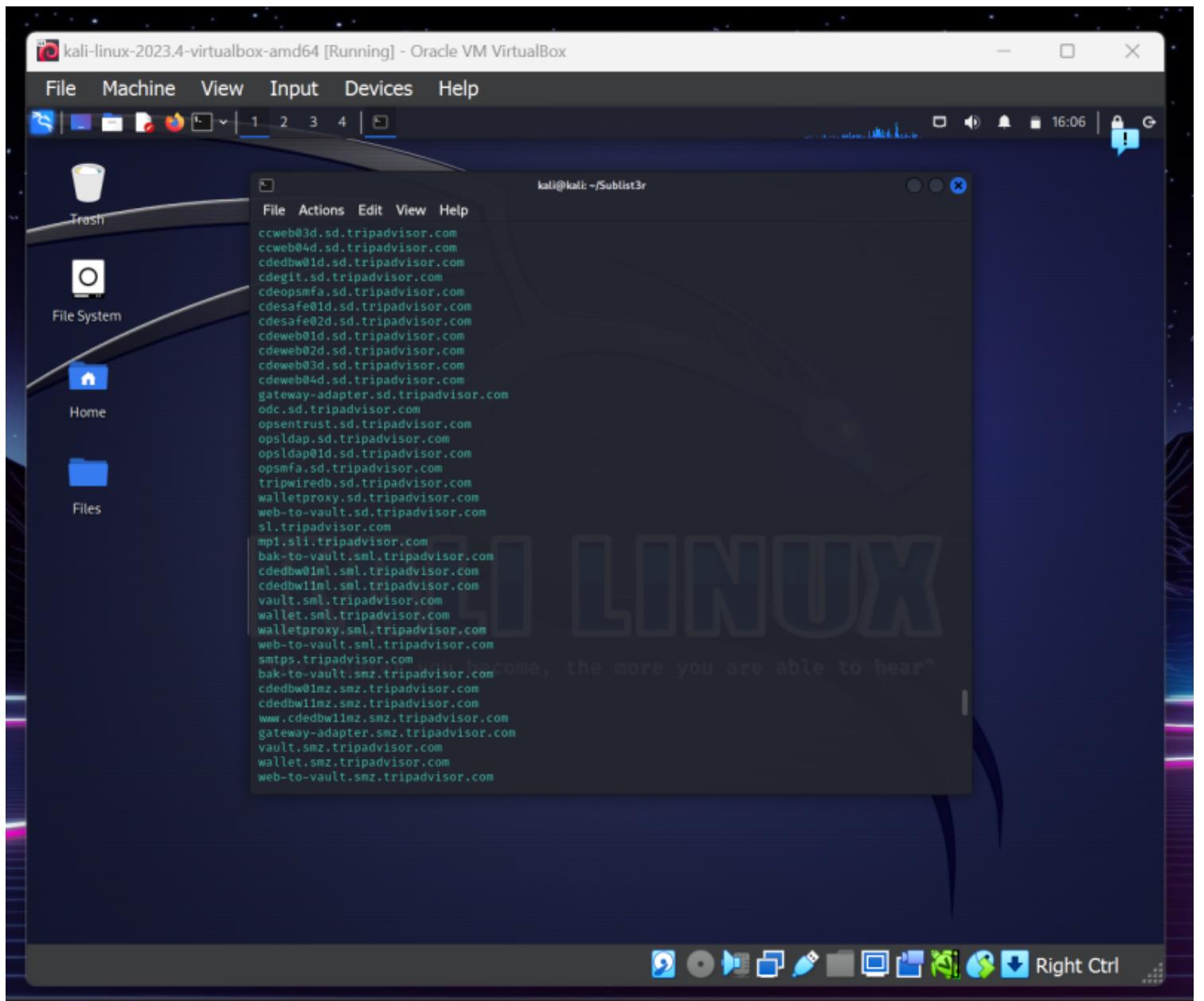
Sublist3r is a tool used to discover subdomains associated with a given domain. It achieves this by querying public DNS servers and scraping search engine results.



```
kali@kali: ~/Sublist3r
$ python sublist3r.py -d tripadvisor.com

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for tripadvisor.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 485
www.tripadvisor.com
911.tripadvisor.com
livesite-docker.a.tripadvisor.com
livesite-maven.a.tripadvisor.com
maven-proxy01a.a.tripadvisor.com
maven-proxy02a.a.tripadvisor.com
opsentrust.a.tripadvisor.com
opsldap.a.tripadvisor.com
opsldap12a.a.tripadvisor.com
opsradius.a.tripadvisor.com
opsradius12a.a.tripadvisor.com
opsslapd01a.a.tripadvisor.com
opsslapd11a.a.tripadvisor.com
```



- 2) Shodan captures information that may include subdomain references, providing insights into the subdomains associated with the target domain.

kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

tripadvisor.com - Shodan | + https://www.shodan.io/search?query=tripadvisor.com

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Shodan Maps Images Monitor Developer More...

SHODAN Explore Pricing tripadvisor.com Search Login

TOTAL RESULTS 54

View Report View on Map Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

TOP COUNTRIES

United States 21

Ireland 18

Australia 4

Spain 3

Germany 2

More...

TOP PORTS

Port	Count
443	37
80	10
1234	4
25	3

TOP ORGANIZATIONS

Organization	Count
Amazon Data Services Ireland Limited	16
Amazon Technologies Inc.	10
Web Hosting Canada	4

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

Cofradía de vinos Solar de Samaniego (IP: 1.1.209.18) (Belgium)

Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 24 Feb 2024 10:17:01 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Set-Cookie: PHPSESSID=d81c4f7291191e9gh4q22xlor2; expires=Sun, 23-Jun-2024 10:17:01 GMT; Max-Age=...

Webcompanion Login (IP: 1.1.209.18) (Belgium)

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate
Content-Security-Policy: worker-src blob:; frame-ancestors 'self'; img-src 'self' blob: data: *.tripadvisor.com; default-src *; style...

Équipements et produits pour érablière, cabane à sucre (IP: 67.23.26.22)

HTTP/1.1 200 OK
Date: Sat, 24 Feb 2024 07:55:32 GMT
Server: Apache

Right Ctrl

Search

1:47 PM 2/24/2024

Emails

1) Hunter.io collects emails associated with the tripadvisor.com domain by collecting data publicly available such as website contact pages, social media profiles, and other online repositories.

Domain Search

tripadvisor.com 246 results Filters

246 results for your search

Jess Findlay jfindlay@tripadvisor.com 94% Save as lead Add to a campaign 1 source

Scott Coufield scoufield@tripadvisor.com 94% Save as lead Add to a campaign 8 sources

Jane Owen jowen@tripadvisor.com 94% Save as lead Add to a campaign 5 sources

Samuel Johns sjohns@tripadvisor.com 94% Save as lead Add to a campaign 2 sources

Inma Solis isolis@tripadvisor.com 94% Save as lead Add to a campaign 8 sources

Tara Lieberman tlieberman@tripadvisor.com 94% Save as lead Add to a campaign 11 sources

Company

Tripadvisor

Plan your next trip, read reviews and get travel advice from our community on where to stay and what to do. Find savings on hot... [more](#)

Email pattern: (f|j|s|t)@tripadvisor.com
Accept all: YES
Industry: Software Development
Headcount: 1001-5000
Address: Needham, Massachusetts, United States

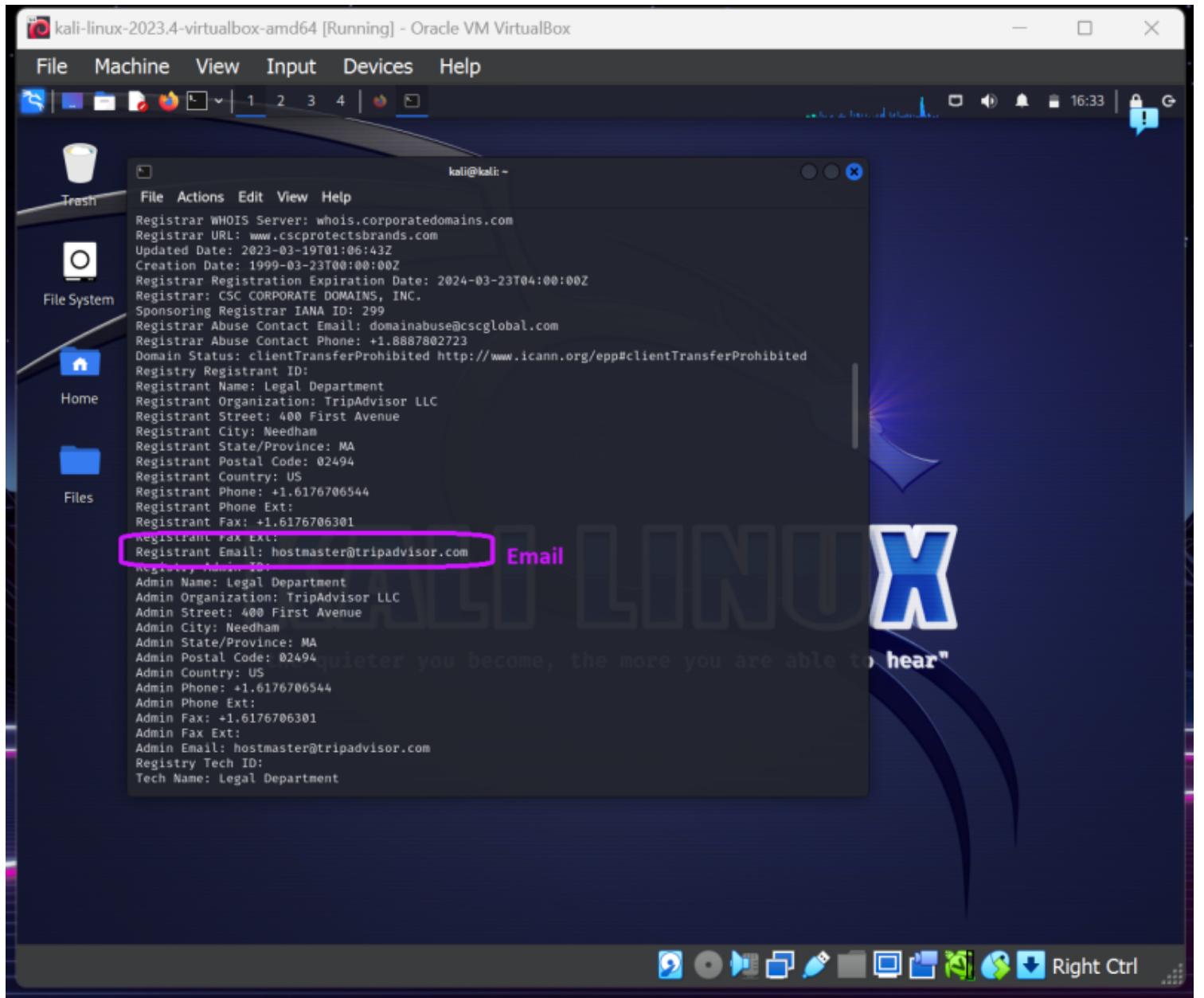
Technologies

iRegarding the pattern of emails:

Naming Convention: All emails start with first initial and end with last name.

They all have the same domain, there's no variation in subdomains.

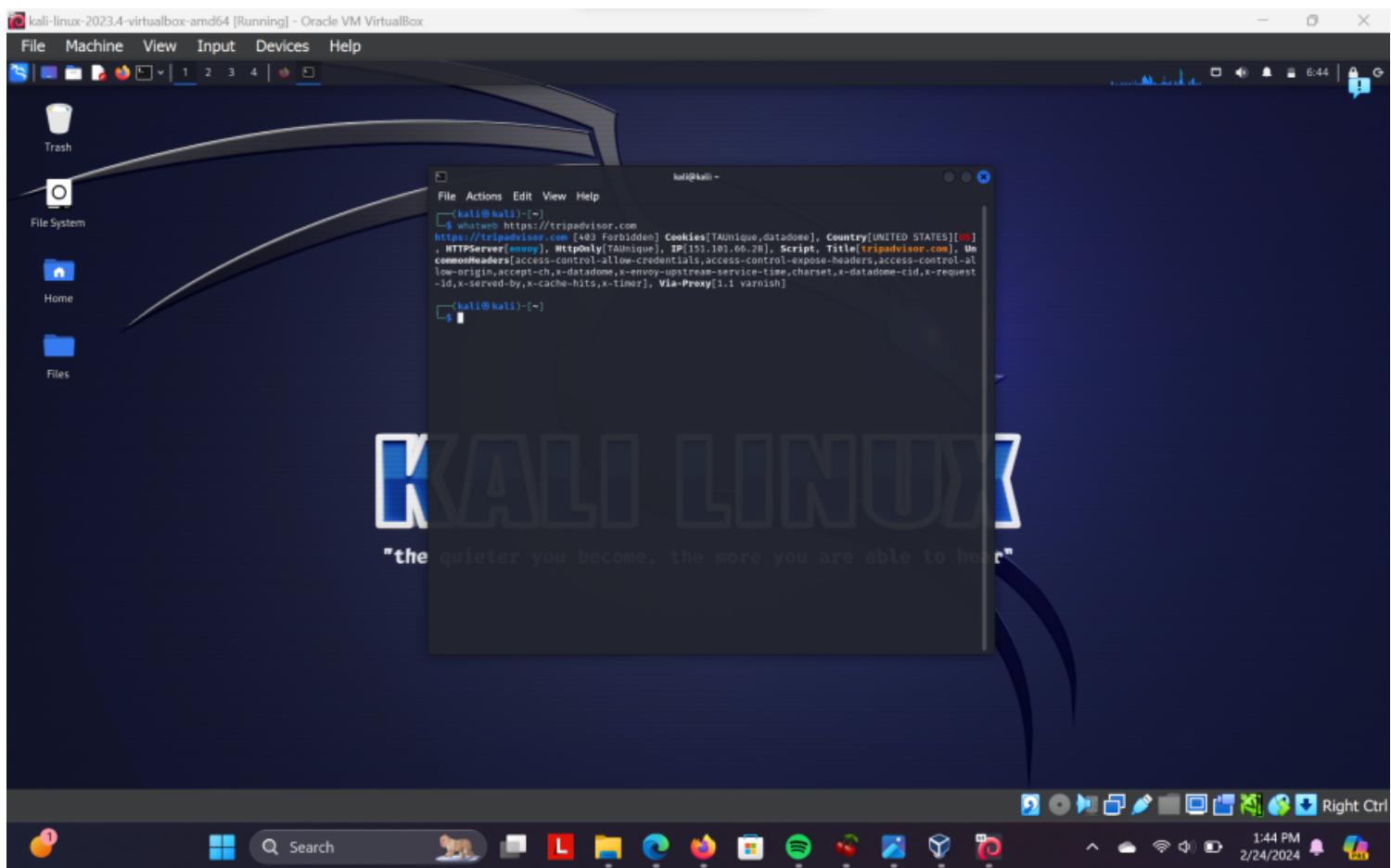
Additional context or metadata alongside email addresses, such as the profession or role associated with the email address was found (CEO, COO, CMO & Interactive Media)



2) When using whois tripadvisor.com

i There was a Role-based email : hostmaster@tripadvisor.com → commonly associated with technical inquiries and administrative matters related to the domain tripadvisor.com.

Domain Fingerprint



- 1) WhatWeb investigates several aspects of the web server, including HTTP headers, HTML markup, JavaScript libraries, and CSS stylesheets. WhatWeb creates a domain fingerprint by analyzing this data, which includes information about the web server software, programming languages, content management systems (CMS), web frameworks, and other technologies used to build and maintain the website.
- 2) Using Wappyzer.com, it collects domain fingerprints for tripadvisor.com by analyzing various aspects of the website's structure, including HTTP headers, HTML markup, JavaScript libraries, CSS stylesheets, and other elements.

The screenshot shows a Kali Linux desktop environment with a browser window open to <https://www.wappalyzer.com/lookup/tripadvisor.com>. The Wappalyzer interface displays the technology stack used by tripadvisor.com, including Zendesk for documentation, Zendesk for issue trackers, Apple iCloud Mail for webmail, Facebook Login and Google Sign-in for authentication, and Cloudflare for reverse proxies. The 'About' section on the right shows options to sign up for Plus features like company and contact details inclusion.

A screenshot of a Kali Linux desktop environment. The main focus is a Firefox browser window displaying the results of a Wappalyzer scan for the website tripadvisor.com. The results are categorized into several sections: Reverse proxies (Envoy), JavaScript frameworks (RxJS, MoTools), Advertising (Prebid, Amazon Advertising, Rubicon Project, Google Publisher Tag, Google Ads), Analytics (Google Analytics (GA4)), and CDN (Akamai). The browser's address bar shows the URL https://www.wappalyzer.com/lookup/tripadvisor.com/. The desktop background is a standard Kali Linux wallpaper. The taskbar at the bottom contains icons for various Kali Linux tools such as Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The system tray on the right shows icons for battery status, signal strength, and system notifications.

A screenshot of a web browser window titled "kali-linux-2023.4-virtualbox-smd164 [Running] - Oracle VM VirtualBox". The address bar shows the URL "https://www.wappalyzer.com/lookup/tripadvisor.com/". The page content is a detailed report from Wappalyzer about the technologies used on tripadvisor.com. Key sections include:

- Cookie compliance:** OneTrust
- Customer data platform:** Segment
- JavaScript libraries:** web-vitals, jQuery (1.12.4)
- Live chat:** Zendesk
- Marketing automation:** Salesforce Marketing Cloud Account Engagement
- Performance:** Priority Hints
- Company size:** 1000-10000 employees
- Company type:** Listed Company
- Social media accounts:** LinkedIn (two entries, one redacted)
- Signals:** Technology spend

The browser interface includes a toolbar with icons for file operations, a tab bar with "Domain Search" and "Technologies used on trip", and a system tray at the bottom.

The screenshot shows a web browser window with the URL <https://www.wappalyzer.com/lookup/tripadvisor.com/>. The page displays various technologies used by the website, categorized into sections:

- RUM**: Includes `web-vitals`.
- Security**: Includes `Akamai Bot Manager`, `DataDome`, `reCAPTCHA`, and `Bugcrowd`.
- Tag managers**: Includes `Google Tag Manager`.
- Miscellaneous**: Includes `Open Graph` and `HTTP/2`.
- Technology spend**: Shows a green bar chart.
- Locale**: Shows `Country: United States`, `Countries: United States`, and `Languages: English`.
- Security**: Shows `SSL/TLS enabled` with a green checkmark.
- Keywords**: Shows a list of keywords: `trip island national tripadvisor tour york content create accessibility choice adult statement ubud book city seller travelers food beach travel`.