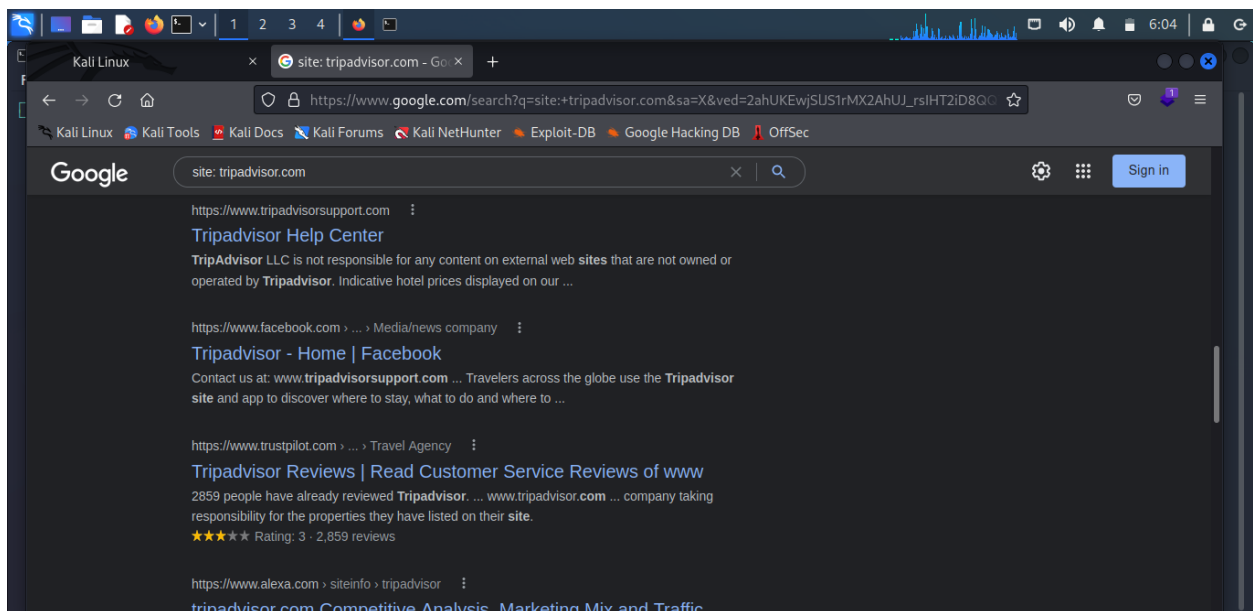
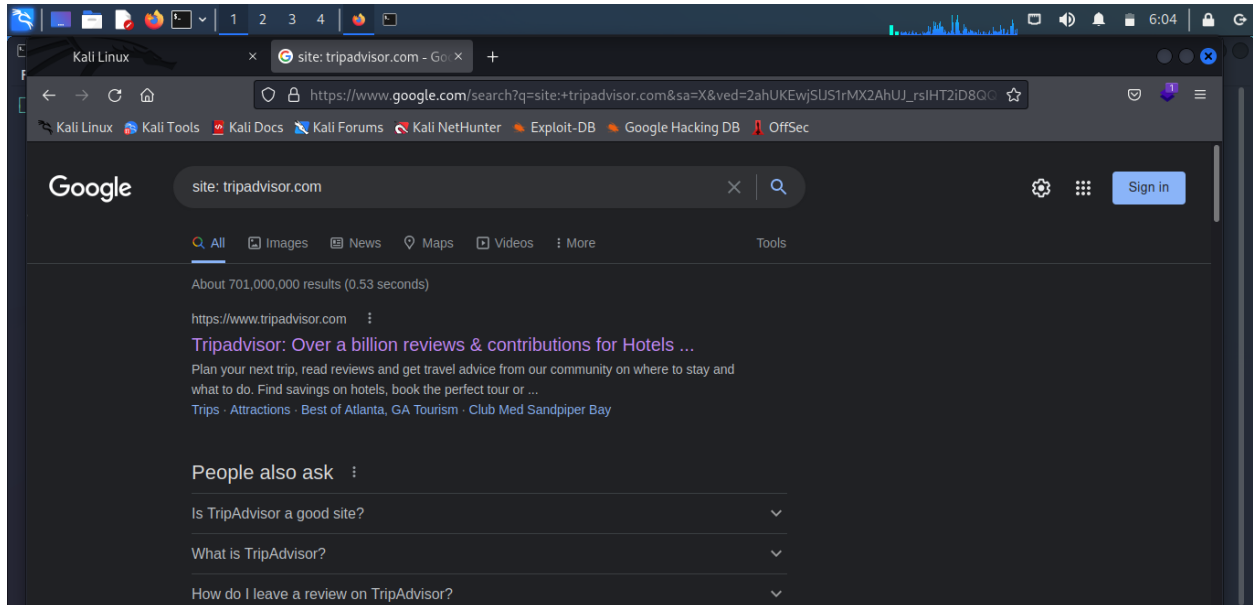


Assignment 1 ETHICAL HACKING

First, we search for site:tripadvisor.com on google to get all the details regarding this website.



Then we open kali linux and open terminal then type the command su saiff to become my user on kali linux and then type the command whois followed by the website we are searching for to get this data about it

```
saiff@kali: /home/kali
File Actions Edit View Help
(kali@kali)-[~]
$ su saiff
Password:
(saiff@kali)-[/home/kali]
$ whois tripadvisor.com
Domain Name: TRIPADVISOR.COM
Registry Domain ID: 4596977_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdns.com
Updated Date: 2020-03-19T05:30:33Z
Creation Date: 1999-03-23T05:00:00Z
Registry Expiry Date: 2022-03-23T04:00:00Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8887802723
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: DNS1.P08.NSONE.NET
Name Server: DNS2.P08.NSONE.NET
Name Server: DNS3.P08.NSONE.NET
Name Server: DNS4.P08.NSONE.NET
Name Server: PDNS1.ULTRADNS.NET
Name Server: PDNS2.ULTRADNS.NET
Name Server: PDNS3.ULTRADNS.ORG
Name Server: PDNS4.ULTRADNS.ORG
Name Server: PDNS5.ULTRADNS.INFO
Name Server: PDNS6.ULTRADNS.CO.UK
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-03-14T10:12:35Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
```

```
saiff@kali: /home/kali
File Actions Edit View Help
NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
```

```
Domain Name: tripadvisor.com
Registry Domain ID: 4596977_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2020-10-21T11:14:55Z
Creation Date: 1999-03-23T00:00:00.000-04:00
Registrar Registration Expiration Date: 2022-03-23T00:00:00.000-04:00
Registrar: CSC CORPORATE DOMAINS, INC.
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 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
Tech Organization: TripAdvisor LLC
Tech Street: 400 First Avenue
Tech City: Needham
Tech State/Province: MA
Tech Postal Code: 02494
Tech Country: US
Tech Phone: +1.6176706544
Tech Phone Ext:
Tech Fax: +1.6176706301
Tech Fax Ext:
Tech Email: hostmaster@tripadvisor.com
Name Server: dns1.p08.nsone.net
Name Server: dns2.p08.nsone.net
Name Server: dns3.p08.nsone.net
Name Server: dns4.p08.nsone.net
Name Server: pdns1.ultradns.net
Name Server: pdns2.ultradns.net
Name Server: pdns3.ultradns.org
Name Server: pdns4.ultradns.org
Name Server: pdns5.ultradns.info
Name Server: pdns6.ultradns.co.uk
DNSSEC: unsigned

For more information on Whois status codes, please visit https://icann.org/epp

Corporation Service Company(c) (CSC) The Trusted Partner of More than 50% of the 100 Best Global Brands.
```

```
saiff@kali: /home/kali
File Actions Edit View Help
Tech Fax: +1.6176706301
Tech Fax Ext:
Tech Email: hostmaster@tripadvisor.com
Name Server: dns1.p08.nsonone.net
Name Server: dns2.p08.nsonone.net
Name Server: dns3.p08.nsonone.net
Name Server: dns4.p08.nsonone.net
Name Server: pdns1.ultradns.net
Name Server: pdns2.ultradns.net
Name Server: pdns3.ultradns.org
Name Server: pdns4.ultradns.org
Name Server: pdns5.ultradns.info
Name Server: pdns6.ultradns.co.uk
DNSSEC: unsigned

For more information on Whois status codes, please visit https://icann.org/epp

Corporation Service Company(c) (CSC) The Trusted Partner of More than 50% of the 100 Best Global Brands.

Contact us to learn more about our enterprise solutions for Global Domain Name Registration and Management, Trademark Research and Watching, Brand, Logo and Auction M
onitoring, as well SSL Certificate Services and DNS Hosting.

NOTICE: You are not authorized to access or query our WHOIS database through the use of high-volume, automated, electronic processes or for the purpose or purposes of
using the data in any manner that violates these terms of use. The Data in the CSC WHOIS database is provided by CSC for information purposes only, and to assist per
sons in obtaining information about or related to a domain name registration record. CSC does not guarantee its accuracy. By submitting a WHOIS query, you agree to ab
ide by the following terms of use: you agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow
, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, e-mail, telephone, or facsimile; or (2) e
nable high volume, automated, electronic processes that apply to CSC (or its computer systems). CSC reserves the right to terminate your access to the WHOIS database
in its sole discretion for any violations by you of these terms of use. CSC reserves the right to modify these terms at any time.

Register your domain name at http://www.cscglobal.com

(saiff@kali)-[/home/kali]
$
```

Then we save the data in ethical1.txt using command `whois tripadvisor.com > ethical1.txt`

And then run the command `nslookup tripadvisor.com` to find out the corresponding IP address or domain name system DNS record.

```
kali@kali: ~
File Actions Edit View Help

(saiff@kali)-[/home/kali]
$ whois tripadvisor.com > ethical1.txt
bash: ethical1.txt: Permission denied

(saiff@kali)-[/home/kali]
$ sudo su
[sudo] password for saiff:
saiff is not in the sudoers file. This incident will be reported.

(saiff@kali)-[/home/kali]
$ su kali
Password:
(kali@kali)-[~]
$ whois tripadvisor.com > ethical1.txt

(kali@kali)-[~]
$ nslookup tripadvisor.com
Server: 163.121.128.134
Address: 163.121.128.134#53

Non-authoritative answer:
Name: tripadvisor.com
Address: 151.101.66.28
Name: tripadvisor.com
Address: 151.101.130.28
Name: tripadvisor.com
Address: 151.101.194.28
Name: tripadvisor.com
Address: 151.101.2.28

(kali@kali)-[~]
$
```

Then we save it in ethical1.txt as well using this command `nslookup tripadvisor.com >> ethical1.txt`

```

kali@kali: ~
└─$ python3 /usr/lib/python3/dist-packages/sublist3r.py [Options] use -h for help
Error: the following arguments are required: -d/--domain

(kali@kali)-[~]
└─$ sublist3r -d tripadvisor.com

Sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la

Usage: python3 /usr/lib/python3/dist-packages/sublist3r.py [Options] use -h for help
Error: the following arguments are required: -d/--domain

(kali@kali)-[~]
└─$ sublist3r -d tripadvisor.com

Sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la

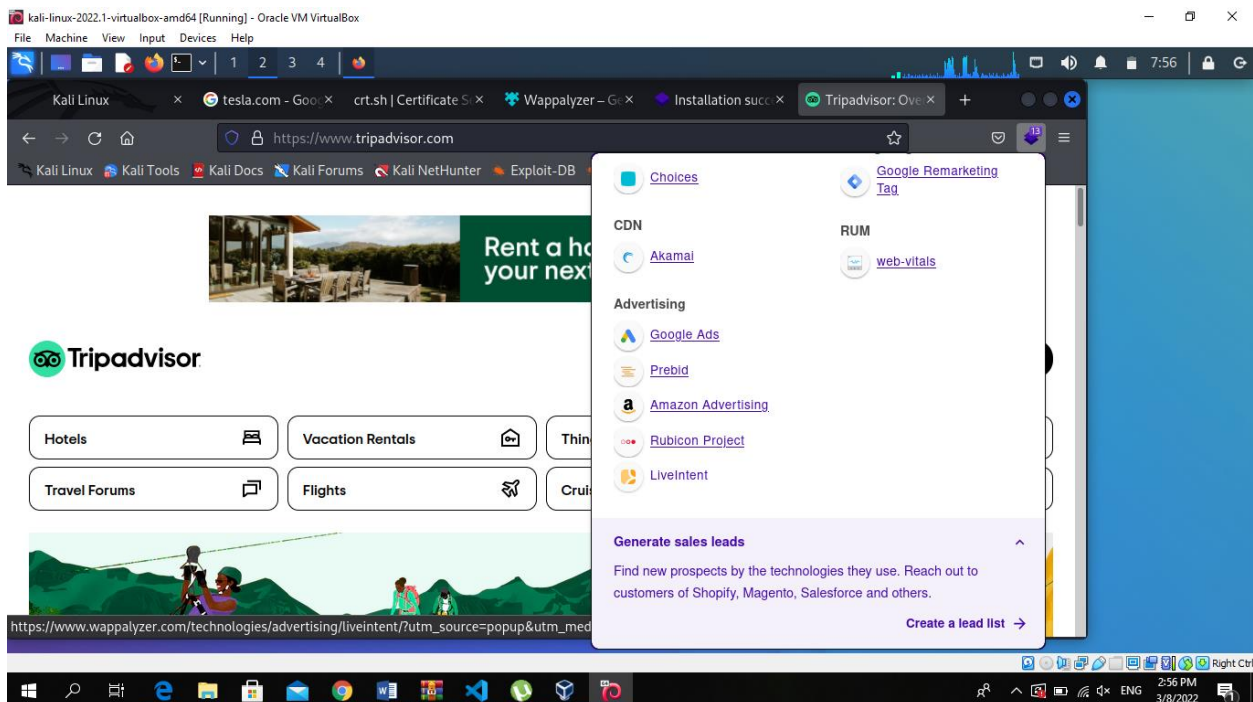
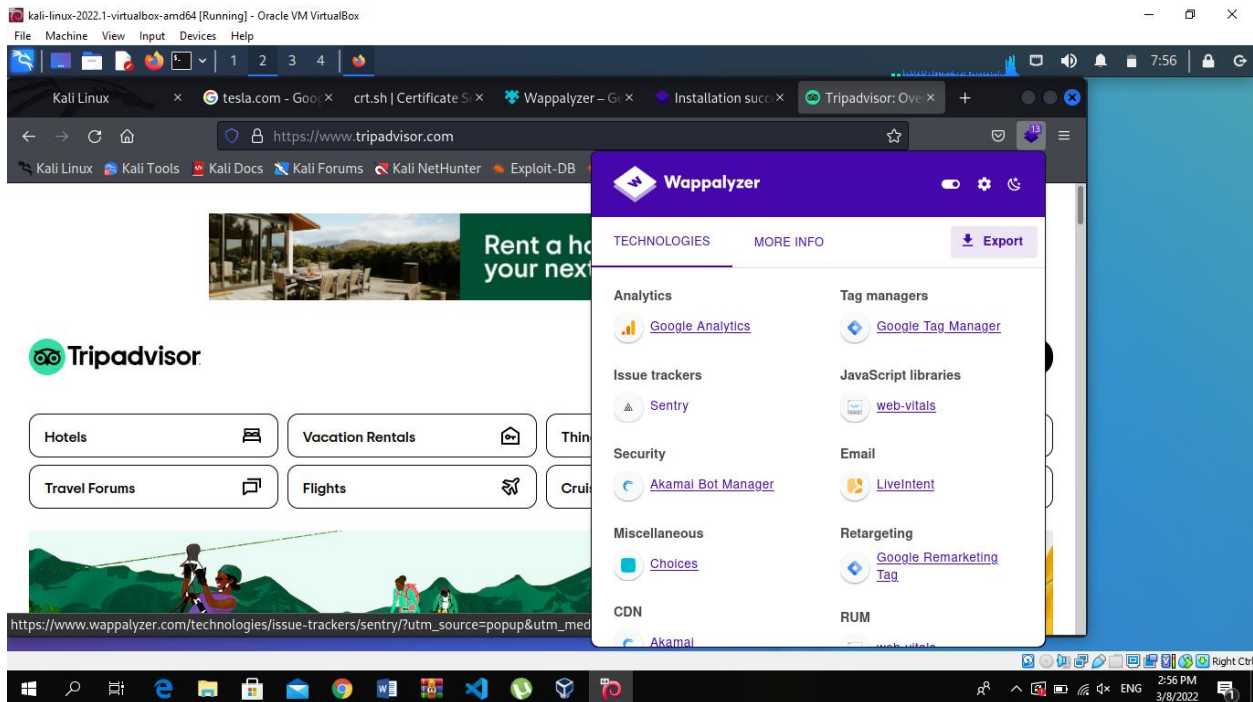
[-] Enumerating subdomains now for tripadvisor.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSDumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
  
```

```
kali@kali: ~  
File Actions Edit View Help  
[~] 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: 301  
www.tripadvisor.com  
mail01a.a.tripadvisor.com  
mail02a.a.tripadvisor.com  
opshtrpb.a.tripadvisor.com  
accor.tripadvisor.com  
activate.tripadvisor.com  
adm01b.tripadvisor.com  
adm02a.tripadvisor.com  
adm02b.tripadvisor.com  
adwww.tripadvisor.com  
affiliates.tripadvisor.com  
airfarewatchdog.tripadvisor.com  
api.tripadvisor.com  
api-bing.tripadvisor.com  
api1-tapayments-com.tripadvisor.com  
api2-tapayments-com.tripadvisor.com  
ar.tripadvisor.com  
arizonaguide.tripadvisor.com  
autodiscover.tripadvisor.com  
ip-199-102-234-105.b.tripadvisor.com  
ip-199-102-234-106.b.tripadvisor.com  
ip-199-102-234-107.b.tripadvisor.com  
ip-199-102-234-108.b.tripadvisor.com  
ip-199-102-234-109.b.tripadvisor.com  
ip-199-102-234-110.b.tripadvisor.com  
ip-199-102-234-113.b.tripadvisor.com  
ip-199-102-234-114.b.tripadvisor.com  
ip-199-102-234-115.b.tripadvisor.com
```

Then we run command whatweb to identify and recognize all the web technologies available on the target website

```
kali@kali: ~  
File Actions Edit View Help  
travelocity.tripadvisor.com  
tripwow.tripadvisor.com  
tuiuk.tripadvisor.com  
massix-ndh.tws.tripadvisor.com  
mail01v.v.tripadvisor.com  
mail02v.v.tripadvisor.com  
vcs-expwy01.tripadvisor.com  
vcs-ext.tripadvisor.com  
virtualtourist.tripadvisor.com  
visittlondon.tripadvisor.com  
visitscotland.tripadvisor.com  
vrt.tripadvisor.com  
walletproxy-tapayments-com.tripadvisor.com  
walletproxy1-tapayments-com.tripadvisor.com  
walletproxy2-tapayments-com.tripadvisor.com  
webmail.tripadvisor.com  
wfh.tripadvisor.com  
widgets.tripadvisor.com  
worldhotels.tripadvisor.com  
  
[kali@kali]~  
$ sublist3r -d tripadvisor.com >> ethical1.txt  
  
[kali@kali]~  
$ whatweb tripadvisor.com  
http://tripadvisor.com [301 Moved Permanently] Country[UNITED STATES][us], HTTPServer[envoy], IP[151.101.2.28], RedirectLocation[https://www.tripadvisor.com/], UncommonHeaders[timing-allow-origin,x-served-by,x-cache-hits,x-timer], Via-Proxy[1.1 varnish]  
https://www.tripadvisor.com/ [200 OK] Bootstrap, Cookies[PAC,PMC,SRT,ServerPool,TADCID,TART,TASID,TASSK,TASession,TATravelInfo,TAUD,TAUnique], Country[UNITED STATES][us], Email[homfeb2022_dt02x.webp,homfeb2022_mm02x.webp,homfeb2022_mm_portrait02x.webp,homfeb2022_tw02x.webp], HTML5, HTTPServer[envoy], HttpOnly[PAC,PMC,TADCID,TART,TASSK,TAUnique], IP[23.46.165.162], Open-Graph-Protocol[website][100000982334629][102749813767076], Script[application/ld+json], Title[Tripadvisor: Over a billion reviews & contributions for Hotels, Attractions, Restaurants, and more], UncommonHeaders[link,timing-allow-origin]  
  
[kali@kali]~  
$
```


Then we use the wappalyzer tool on tripadvisor.com to get us what websites are built with. Find out what CMS a website is using, and the frameworks as well as ecommerce platform and JavaScript libraries



We then use crt.sh which is an online tool to get all the TLS and SSL certificates of tripadvisor.com domain

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Kali Linux crt.sh | tripadvisor.com

https://crt.sh/?q=tripadvisor.com

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

crt.sh Identity Search [Group by Issuer](#)

Criteria Type: Identity Match: ILIKE Search: 'tripadvisor.com'

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	6326364209	2022-03-12	2022-03-12	2022-06-10	business.tripadvisor.com	business.tripadvisor.com	C=US, O=Let's Encrypt, CN=R3
	6326364298	2022-03-12	2022-03-12	2022-06-10	business.tripadvisor.com	business.tripadvisor.com	C=US, O=Let's Encrypt, CN=R3
	6323112887	2022-03-11	2022-03-11	2023-03-22	hare.tripadvisor.com	activate.mz.tripadvisor.com hare-api.tripadvisor.com hare-ar.tripadvisor.com hare-cdn.tripadvisor.com hare-cn.tripadvisor.com hare-en.tripadvisor.com.hk hare-no.tripadvisor.com hare-pl.tripadvisor.com hare-th.tripadvisor.com hare.tripadvisor.com hare.tripadvisor.com.ar hare.tripadvisor.com.au hare.tripadvisor.com.br hare.tripadvisor.com.eg hare.tripadvisor.com.gr hare.tripadvisor.com.hk hare.tripadvisor.com.mx hare.tripadvisor.com.my hare.tripadvisor.com.pe hare.tripadvisor.com.ph	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1

7:39 PM 3/12/2022

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Kali Linux crt.sh | tripadvisor.com

https://crt.sh/?q=tripadvisor.com

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

6280159258	2022-03-04	2022-03-04	2023-04-04	tripwiredb.sb.tripadvisor.com	hare.tripadvisor.com.vn tripwiredb.sb.tripadvisor.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6277605479	2022-03-03	2022-03-03	2023-04-04	tripwiredb.sd.tripadvisor.com	tripwiredb.sd.tripadvisor.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018
6260310148	2022-02-28	2022-02-28	2023-02-28	security.tools.tripadvisor.com	sec11d.d.tripadvisor.com sec12d.d.tripadvisor.com security.tools.tripadvisor.com tools-security.tripadvisor.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6259198255	2022-02-28	2022-02-28	2023-04-01	careers.tripadvisor.com	careers.tripadvisor.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018
6258635278	2022-02-28	2022-02-28	2023-04-01	tonic.tripadvisor.com	tonic21d.d.tripadvisor.com tonic22d.d.tripadvisor.com tonic.tools.tripadvisor.com tonic.tripadvisor.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018
6257561725	2022-02-28	2021-03-19	2022-04-19	media.tacdn.com	dynamic-media-cdn.tripadvisor.com media-cdn.tripadvisor.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6234501064	2022-02-24	2022-02-24	2022-05-25	join.plus.tripadvisor.com	join.plus.tripadvisor.com	C=US, O=Let's Encrypt, CN=R3
6234494069	2022-02-24	2022-02-24	2022-05-25	join.plus.tripadvisor.com	join.plus.tripadvisor.com	C=US, O=Let's Encrypt, CN=R3
6227053079	2022-02-22	2022-02-22	2022-05-23	products.dtc.tripadvisor.com	products.dtc.tripadvisor.com	C=US, O=Let's Encrypt, CN=R3
6227201388	2022-02-22	2022-02-22	2022-05-23	products.dtc.tripadvisor.com	products.dtc.tripadvisor.com	C=US, O=Let's Encrypt, CN=R3
6219210290	2022-02-21	2022-02-21	2023-03-23	seo.hd.tripadvisor.com	seo.hd.tripadvisor.com seo.hl.tripadvisor.com vrsupply.hd.tripadvisor.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6212208621	2022-02-20	2022-02-20	2022-05-21	products.plus.tripadvisor.com	products.plus.tripadvisor.com	C=US, O=Let's Encrypt, CN=R3
6212252156	2022-02-20	2022-02-20	2022-05-21	products.plus.tripadvisor.com	products.plus.tripadvisor.com	C=US, O=Let's Encrypt, CN=R3
6211713030	2022-02-20	2022-02-16	2023-03-09	dynamic-media-cdn.tripadvisor.com	dynamic-media-cdn.tripadvisor.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6207204426	2022-02-19	2022-02-16	2023-03-09	dynamic-media-cdn.tripadvisor.com	dynamic-media-cdn.tripadvisor.com	C=US, O=DigiCert Inc, CN=DigiCert TLS

7:40 PM 3/12/2022

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Kali Linux crt.sh | tripadvisor.com

https://crt.sh/?q=tripadvisor.com

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

6211713030	2022-02-20	2022-02-16	2023-03-09	dynamic-media-cdn.tripadvisor.com	dynamic-media-cdn.tripadvisor.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6207204426	2022-02-19	2022-02-16	2023-03-09	dynamic-media-cdn.tripadvisor.com	dynamic-media-cdn.tripadvisor.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6197608879	2022-02-17	2022-02-17	2022-05-18	www.purpose.tripadvisor.com	www.purpose.tripadvisor.com	C=US, O=Let's Encrypt, CN=R3
6197608153	2022-02-17	2022-02-17	2022-05-18	www.purpose.tripadvisor.com	www.purpose.tripadvisor.com	C=US, O=Let's Encrypt, CN=R3
6191270463	2022-02-16	2022-02-16	2022-05-17	purpose.tripadvisor.com	purpose.tripadvisor.com	C=US, O=Let's Encrypt, CN=R3
6191259910	2022-02-16	2022-02-16	2022-05-17	purpose.tripadvisor.com	purpose.tripadvisor.com	C=US, O=Let's Encrypt, CN=R3
6189967584	2022-02-16	2022-02-16	2023-03-09	dynamic-media-cdn.tripadvisor.com	dynamic-media-cdn.tripadvisor.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6189800314	2022-02-16	2022-02-16	2023-03-09	dynamic-media-cdn.tripadvisor.com	dynamic-media-cdn.tripadvisor.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6189538912	2022-02-16	2022-02-16	2023-03-09	dynamic-media-cdn.tripadvisor.com	dynamic-media-cdn.tripadvisor.com	C=US, O=DigiCert Inc, CN=DigiCert TLS RSA SHA256 2020 CA1
6158002648	2022-02-11	2022-02-11	2023-03-12	lmt.tripadvisor.com	lmt01d.d.tripadvisor.com lmt02d.d.tripadvisor.com lmt.tools.tripadvisor.com lmt.tripadvisor.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018
6160041894	2022-02-11	2022-02-11	2022-05-12	sl.tripadvisor.com	sl.tripadvisor.com	C=US, O=Let's Encrypt, CN=R3
6153904428	2022-02-11	2022-02-11	2022-05-12	sl.tripadvisor.com	sl.tripadvisor.com	C=US, O=Let's Encrypt, CN=R3
6150432020	2022-02-10	2022-02-10	2023-03-14	wallet.smz.tripadvisor.com	wallet.smz.tripadvisor.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018
6150432048	2022-02-10	2022-02-10	2023-03-14	vault.smz.tripadvisor.com	vault.smz.tripadvisor.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018
6143270063	2022-02-09	2022-02-09	2023-03-13	*.platform.tripadvisor.com	*.emissary.kub.var.a.tripadvisor.com ingress-gateway.platform.a.tripadvisor.com *.platform.a.tripadvisor.com *.platform.tripadvisor.com platform.tripadvisor.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018

Right Ctrl

7:43 PM 3/12/2022