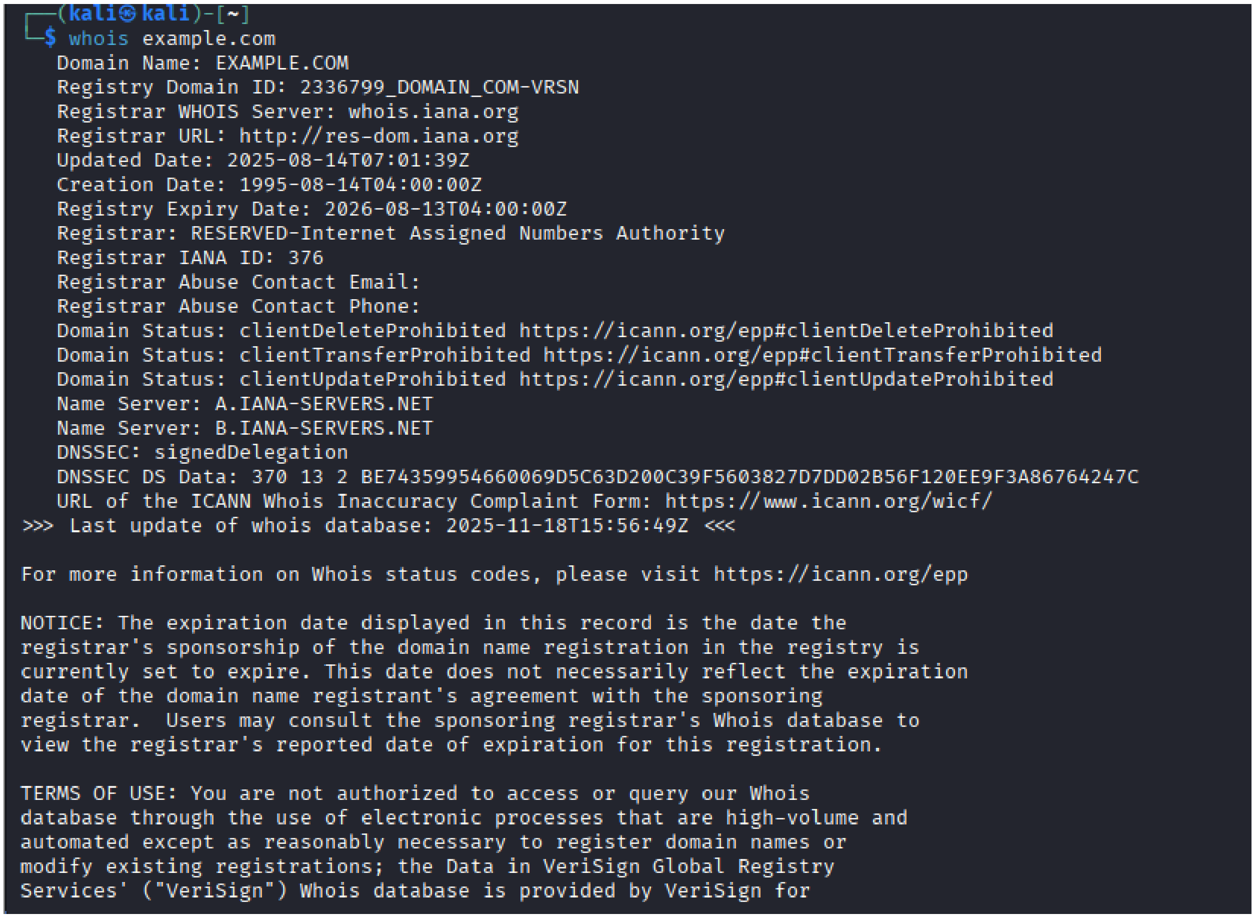
ASSIGNMENT 2- PASSIVE RECON

STEP 1 — Domain Information Gathering

1. WHOIS Lookup

whois example.com



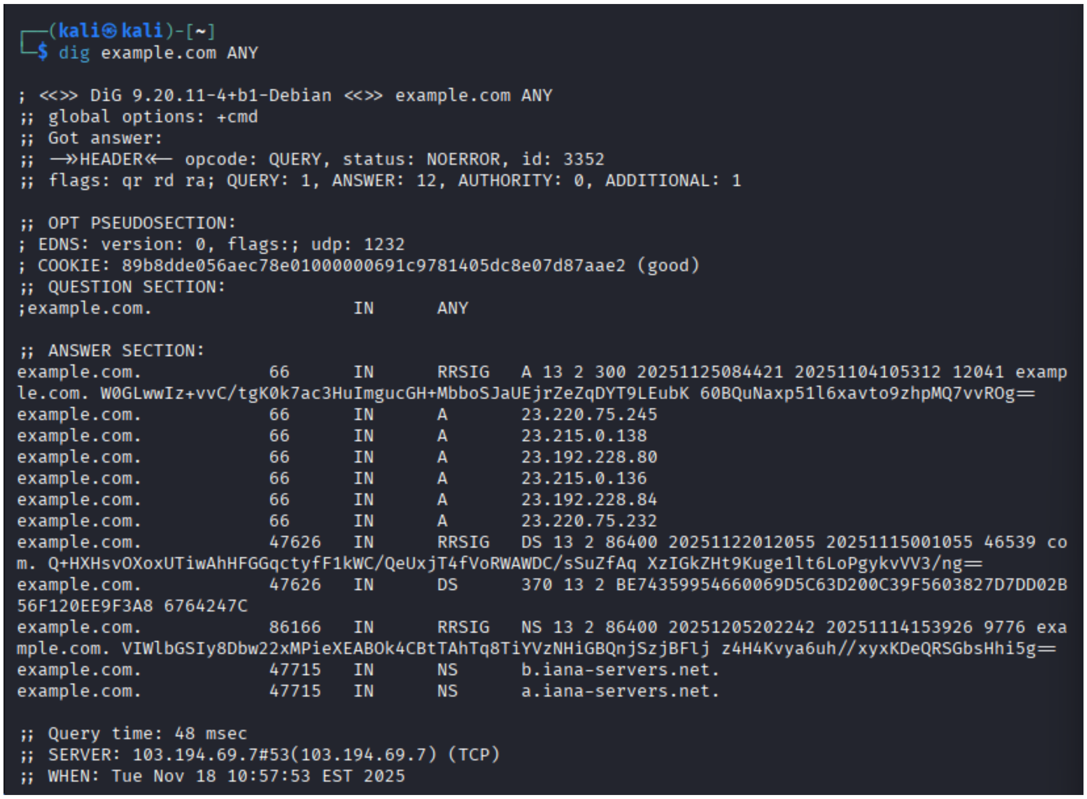
```
┌──(kali㉿kali)-[~]
└─$ whois example.com
   Domain Name: EXAMPLE.COM
   Registry Domain ID: 2336799_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.iana.org
   Registrar URL: http://res-dom.iana.org
   Updated Date: 2025-08-14T07:01:39Z
   Creation Date: 1995-08-14T04:00:00Z
   Registry Expiry Date: 2026-08-13T04:00:00Z
   Registrar: RESERVED-Internet Assigned Numbers Authority
   Registrar IANA ID: 376
   Registrar Abuse Contact Email:
   Registrar Abuse Contact Phone:
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: A.IANA-SERVERS.NET
   Name Server: B.IANA-SERVERS.NET
   DNSSEC: signedDelegation
   DNSSEC DS Data: 370 13 2 BE74359954660069D5C63D200C39F5603827D7DD02B56F120EE9F3A86764247C
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-11-18T15:56:49Z <<<

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
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
```

Collect:

- Registrar
- Domain owner
- Nameservers
- Expiry date
- Contact emails

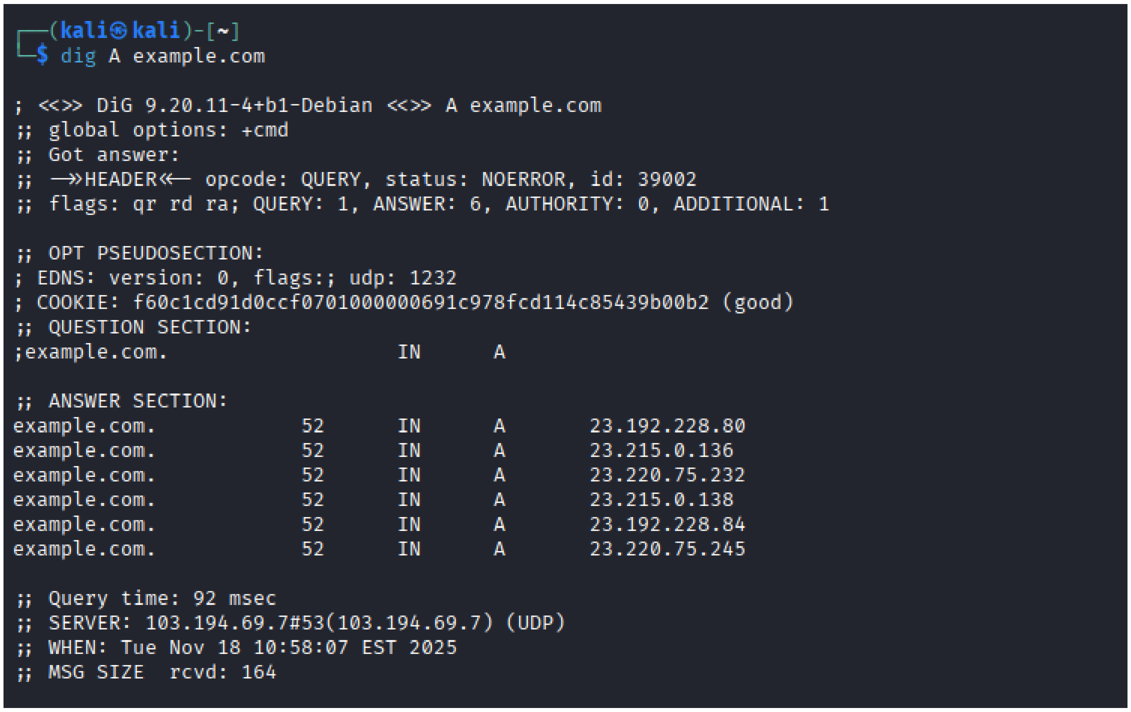
2. DNS Records Using dig

dig example.com ANY



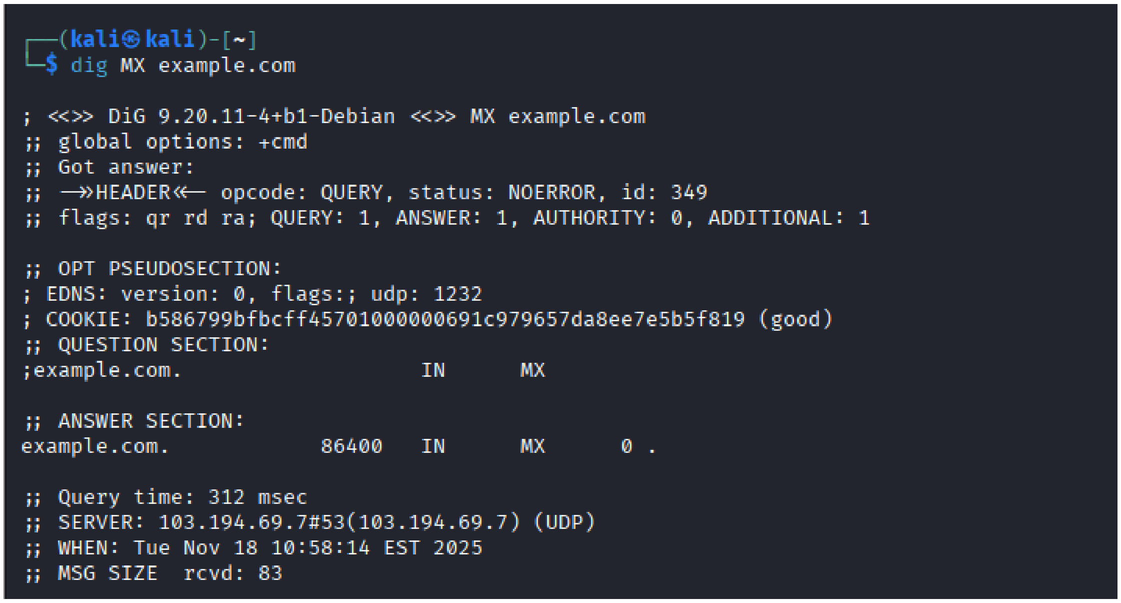
```
┌──(kali㉿kali)-[~]
└─$ dig example.com ANY

; <<>> DiG 9.20.11-4+b1-Debian <<>> example.com ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3352
;; flags: qr rd ra; QUERY: 1, ANSWER: 12, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 89b8dde056aec78e01000000691c9781405dc8e07d87aae2 (good)
;; QUESTION SECTION:
;example.com.                   IN      ANY

;; ANSWER SECTION:
example.com.            66      IN      RRSIG   A 13 2 300 20251125084421 20251104105312 12041 examp
le.com. W0GLwwIz+vvC/tgK0k7ac3HuImgucGH+MbboSJaUEjrZeZqDYT9LEubK 60BQuNaxp51l6xavto9zhpMQ7vvROg==
example.com.            66      IN      A       23.220.75.245
example.com.            66      IN      A       23.215.0.138
example.com.            66      IN      A       23.192.228.80
example.com.            66      IN      A       23.215.0.136
example.com.            66      IN      A       23.192.228.84
example.com.            66      IN      A       23.220.75.232
example.com.            47626   IN      RRSIG   DS 13 2 86400 20251122012055 20251115001055 46539 co
m. Q+HXHsvOXoxUTiwAhHFGGqctyfF1kWC/QeUxjT4fVoRWAWDC/sSuZfAq XzIGkZHt9Kuge1lt6LoPgykvVV3/ng==
example.com.            47626   IN      DS      370 13 2 BE74359954660069D5C63D200C39F5603827D7DD02B
56F120EE9F3A8 6764247C
example.com.            86166   IN      RRSIG   NS 13 2 86400 20251205202242 20251114153926 9776 exa
mple.com. VIWlbGSIy8Dbw22xMPieXEABOk4CBtTAhTq8TiYVzNHiGBQnjSzjBFlj z4H4Kvya6uh//xyxKDeQRSGbsHhi5g==
example.com.            47715   IN      NS      b.iana-servers.net.
example.com.            47715   IN      NS      a.iana-servers.net.

;; Query time: 48 msec
;; SERVER: 103.194.69.7#53(103.194.69.7) (TCP)
;; WHEN: Tue Nov 18 10:57:53 EST 2025
```

dig A example.com



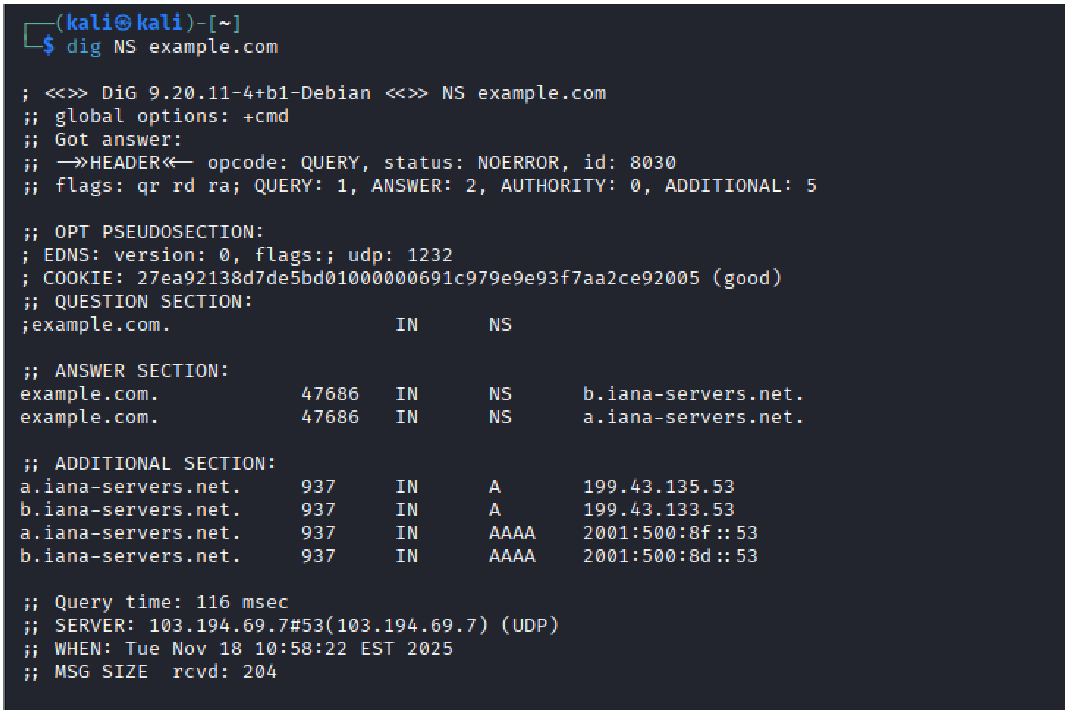
```
┌──(kali㉿kali)-[~]
└─$ dig A example.com

; <<>> DiG 9.20.11-4+b1-Debian <<>> A example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39002
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: f60c1cd91d0ccf0701000000691c978fcd114c85439b00b2 (good)
;; QUESTION SECTION:
;example.com.                   IN      A

;; ANSWER SECTION:
example.com.            52      IN      A       23.192.228.80
example.com.            52      IN      A       23.215.0.136
example.com.            52      IN      A       23.220.75.232
example.com.            52      IN      A       23.215.0.138
example.com.            52      IN      A       23.192.228.84
example.com.            52      IN      A       23.220.75.245

;; Query time: 92 msec
;; SERVER: 103.194.69.7#53(103.194.69.7) (UDP)
;; WHEN: Tue Nov 18 10:58:07 EST 2025
;; MSG SIZE  rcvd: 164
```

dig MX example.com



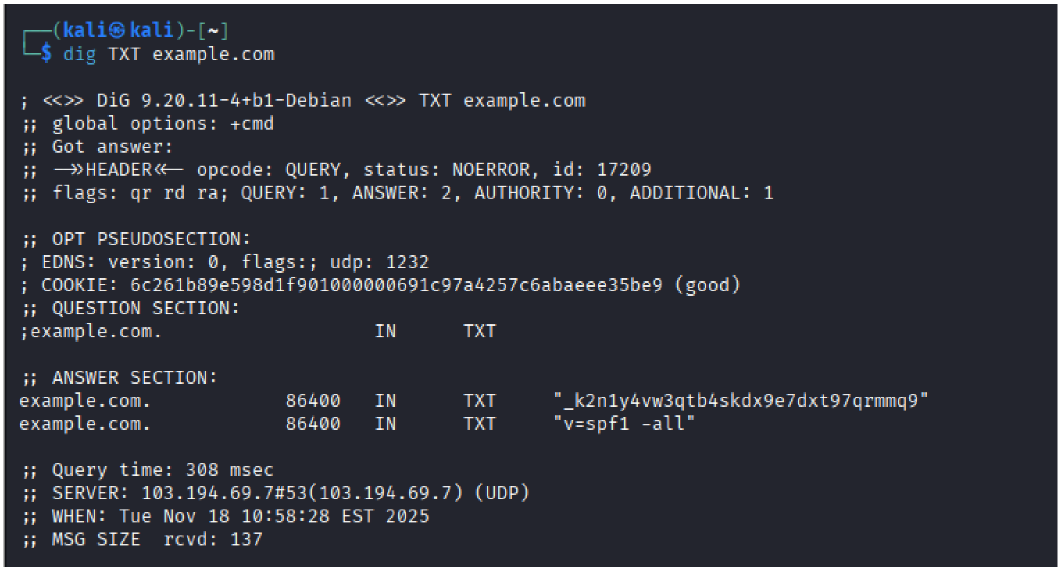
```
┌──(kali㉿kali)-[~]
└─$ dig MX example.com

; <<>> DiG 9.20.11-4+b1-Debian <<>> MX example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 349
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b586799bfbcff45701000000691c979657da8ee7e5b5f819 (good)
;; QUESTION SECTION:
;example.com.                   IN      MX

;; ANSWER SECTION:
example.com.            86400   IN      MX      0 .

;; Query time: 312 msec
;; SERVER: 103.194.69.7#53(103.194.69.7) (UDP)
;; WHEN: Tue Nov 18 10:58:14 EST 2025
;; MSG SIZE  rcvd: 83
```

dig NS example.com



```
┌──(kali㉿kali)-[~]
└─$ dig NS example.com

; <<>> DiG 9.20.11-4+b1-Debian <<>> NS example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8030
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 27ea92138d7de5bd01000000691c979e9e93f7aa2ce92005 (good)
;; QUESTION SECTION:
;example.com.                   IN      NS

;; ANSWER SECTION:
example.com.            47686   IN      NS      b.iana-servers.net.
example.com.            47686   IN      NS      a.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net.     937     IN      A       199.43.135.53
b.iana-servers.net.     937     IN      A       199.43.133.53
a.iana-servers.net.     937     IN      AAAA    2001:500:8f::53
b.iana-servers.net.     937     IN      AAAA    2001:500:8d::53

;; Query time: 116 msec
;; SERVER: 103.194.69.7#53(103.194.69.7) (UDP)
;; WHEN: Tue Nov 18 10:58:22 EST 2025
;; MSG SIZE  rcvd: 204
```

dig TXT example.com

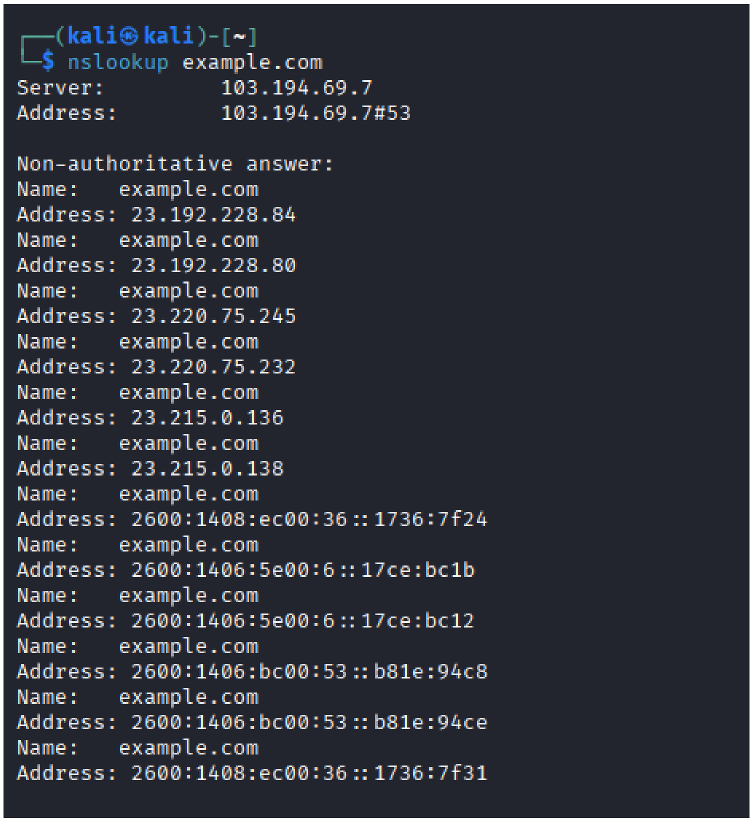


```
┌──(kali㉿kali)-[~]
└─$ dig TXT example.com

; <<>> DiG 9.20.11-4+b1-Debian <<>> TXT example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17209
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 6c261b89e598d1f901000000691c97a4257c6abaeee35be9 (good)
;; QUESTION SECTION:
;example.com.                   IN      TXT

;; ANSWER SECTION:
example.com.            86400   IN      TXT     "_k2n1y4vw3qtb4skdx9e7dxt97qrmmq9"
example.com.            86400   IN      TXT     "v=spf1 -all"

;; Query time: 308 msec
;; SERVER: 103.194.69.7#53(103.194.69.7) (UDP)
;; WHEN: Tue Nov 18 10:58:28 EST 2025
;; MSG SIZE  rcvd: 137
```

---

3. DNS Records Using nslookup

nslookup example.com



```
┌──(kali㉿kali)-[~]
└─$ nslookup example.com
Server:         103.194.69.7
Address:        103.194.69.7#53

Non-authoritative answer:
Name:   example.com
Address: 23.192.228.84
Name:   example.com
Address: 23.192.228.80
Name:   example.com
Address: 23.220.75.245
Name:   example.com
Address: 23.220.75.232
Name:   example.com
Address: 23.215.0.136
Name:   example.com
Address: 23.215.0.138
Name:   example.com
Address: 2600:1408:ec00:36::1736:7f24
Name:   example.com
Address: 2600:1406:5e00:6::17ce:bc1b
Name:   example.com
Address: 2600:1406:5e00:6::17ce:bc12
Name:   example.com
Address: 2600:1406:bc00:53::b81e:94c8
Name:   example.com
Address: 2600:1406:bc00:53::b81e:94ce
Name:   example.com
Address: 2600:1408:ec00:36::1736:7f31
```

DNS Resolver Used

- 103.194.69.7 (ISP DNS)

A Records (IPv4 Addresses)

- 23.192.228.84
- 23.192.228.80
- 23.220.75.245
- 23.220.75.232
- 23.215.0.136
- 23.215.0.138

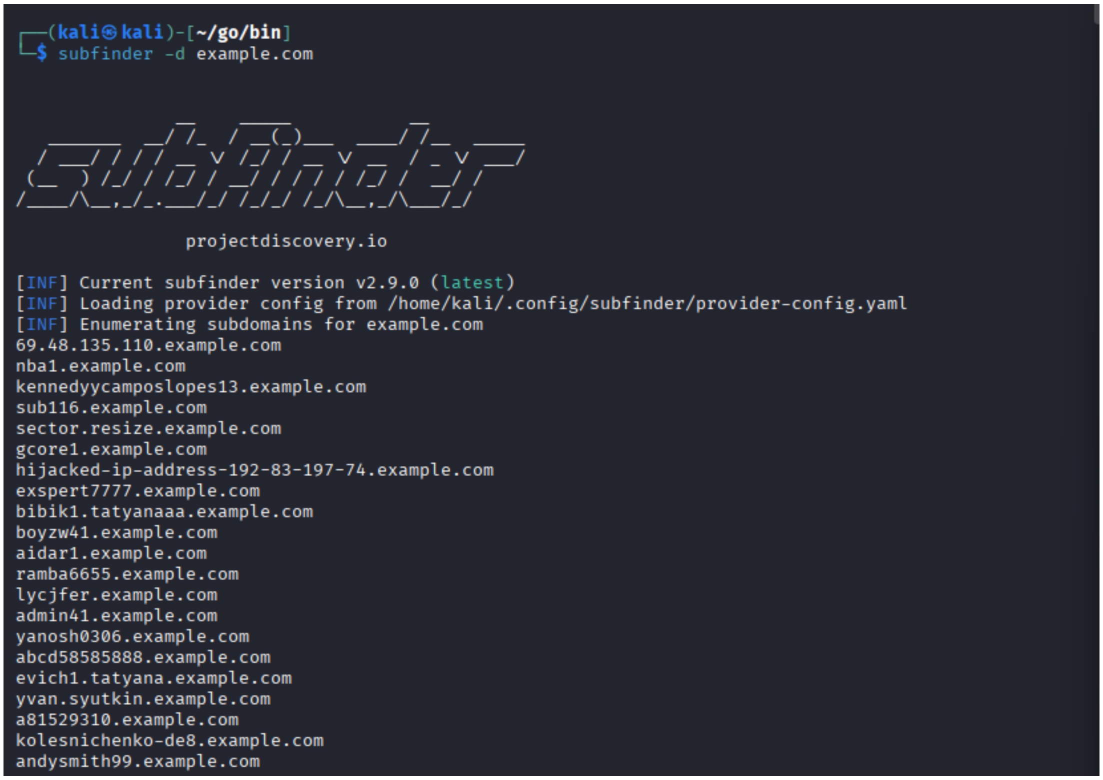
AAAA Records (IPv6 Addresses)

- 2600:1408:ec00:36::1736:7f24
- 2600:1406:5e00:6::17ce:bc1b
- 2600:1406:5e00:6::17ce:bc12
- 2600:1406:bc00:53::b81e:94c8
- 2600:1406:bc00:53::b81e:94ce
- 2600:1408:ec00:36::1736:7f31

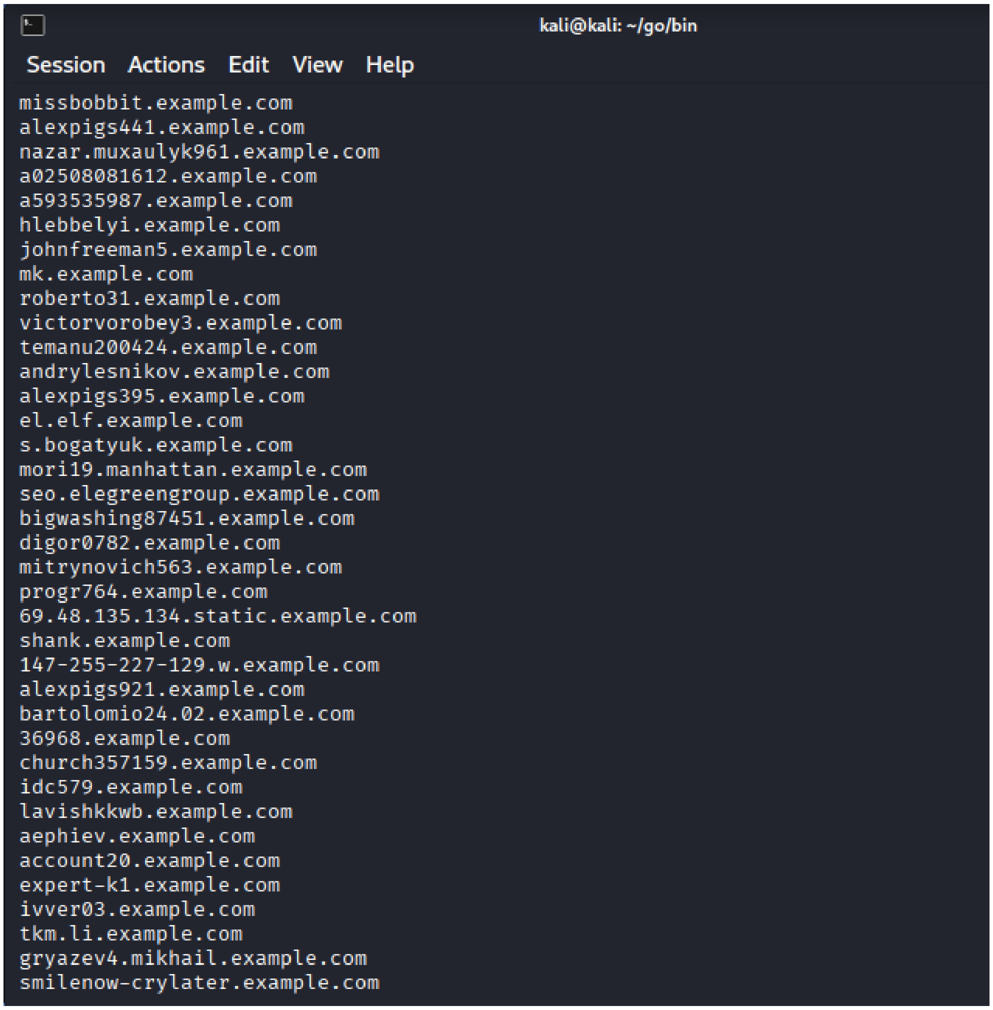
STEP 2 — Passive Subdomain Enumeration

1. Subfinder

subfinder -d example.com -o subdomains.txt



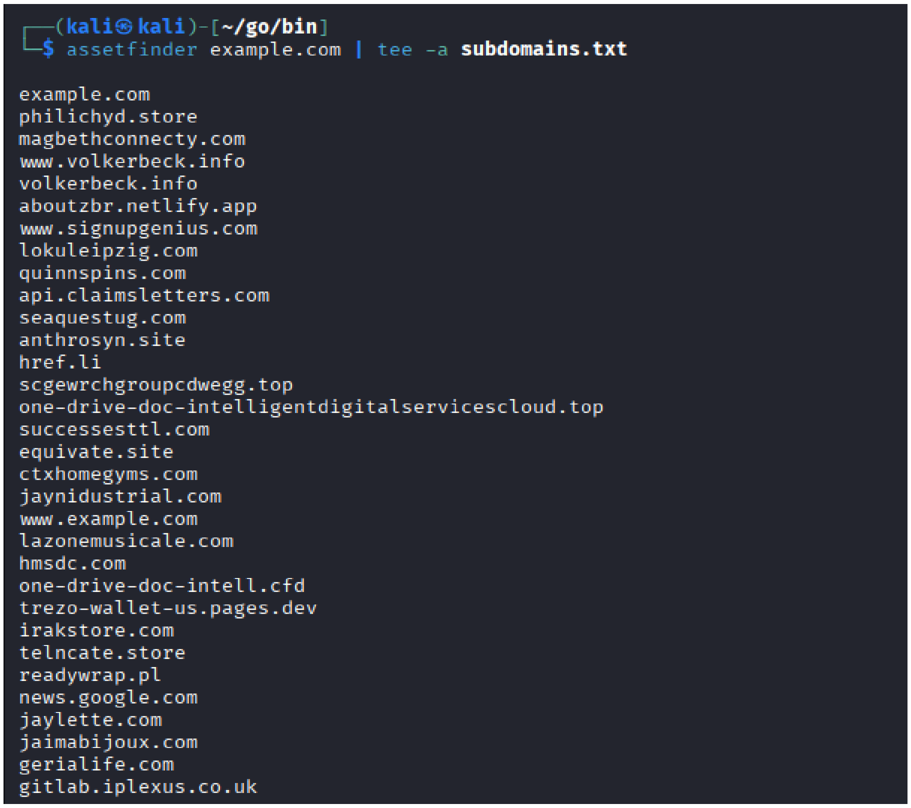
```
┌──(kali㉿kali)-[~/go/bin]
└─$ subfinder -d example.com


               __    _____           __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Current subfinder version v2.9.0 (latest)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for example.com
69.48.135.110.example.com
nba1.example.com
kennedyycamposlopes13.example.com
sub116.example.com
sector.resize.example.com
gcore1.example.com
hijacked-ip-address-192-83-197-74.example.com
exspert7777.example.com
bibik1.tatyanaaa.example.com
boyzw41.example.com
aidar1.example.com
ramba6655.example.com
lycjfer.example.com
admin41.example.com
yanosh0306.example.com
abcd58585888.example.com
evich1.tatyana.example.com
yvan.syutkin.example.com
a81529310.example.com
kolesnichenko-de8.example.com
andysmith99.example.com
```



```
missbobbit.example.com
alexpigs441.example.com
nazar.muxaulyk961.example.com
a02508081612.example.com
a593535987.example.com
hlebbelyi.example.com
johnfreeman5.example.com
mk.example.com
roberto31.example.com
victorvorobey3.example.com
temanu200424.example.com
andrylesnikov.example.com
alexpigs395.example.com
el.elf.example.com
s.bogatyuk.example.com
mori19.manhattan.example.com
seo.elegreengroup.example.com
bigwashing87451.example.com
digor0782.example.com
mitrynovich563.example.com
progr764.example.com
69.48.135.134.static.example.com
shank.example.com
147-255-227-129.w.example.com
alexpigs921.example.com
bartolomio24.02.example.com
36968.example.com
church357159.example.com
idc579.example.com
lavishkkwb.example.com
aephiev.example.com
account20.example.com
expert-k1.example.com
ivver03.example.com
tkm.li.example.com
gryazev4.mikhail.example.com
smilenow-crylater.example.com
```

2. Assetfinder

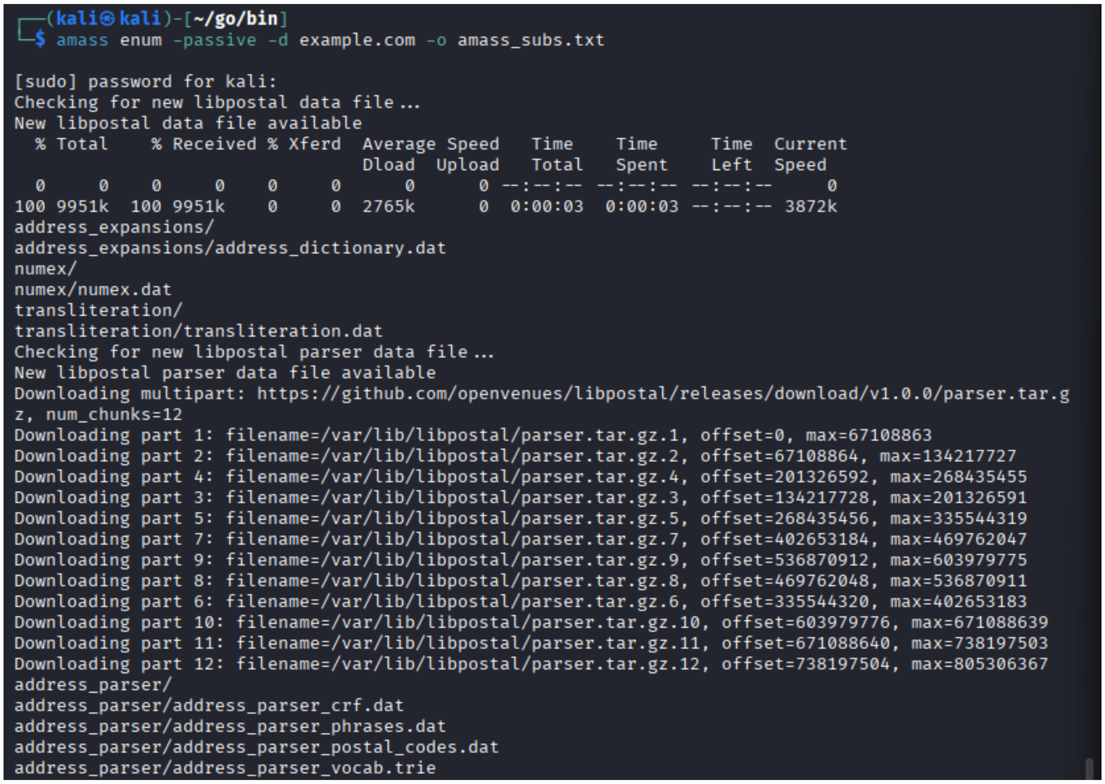
assetfinder example.com | tee -a subdomains.txt



```
┌──(kali㉿kali)-[~/go/bin]
└─$ assetfinder example.com | tee -a subdomains.txt

example.com
philichyd.store
magbethconnecty.com
www.volkerbeck.info
volkerbeck.info
aboutzbr.netlify.app
www.signupgenius.com
lokuleipzig.com
quinnspins.com
api.claimsletters.com
seaquestug.com
anthrosyn.site
href.li
scgewrchgroupcdwegg.top
one-drive-doc-intelligentdigitalservicescloud.top
successesttl.com
equivate.site
ctxhomegyms.com
jaynidustrial.com
www.example.com
lazonemusicale.com
hmsdc.com
one-drive-doc-intell.cfd
trezo-wallet-us.pages.dev
irakstore.com
telncate.store
readywrap.pl
news.google.com
jaylette.com
jaimabijoux.com
gerialife.com
gitlab.iplexus.co.uk
```

3. amass (passive mode)

amass enum -passive -d example.com -o amass_subs.txt



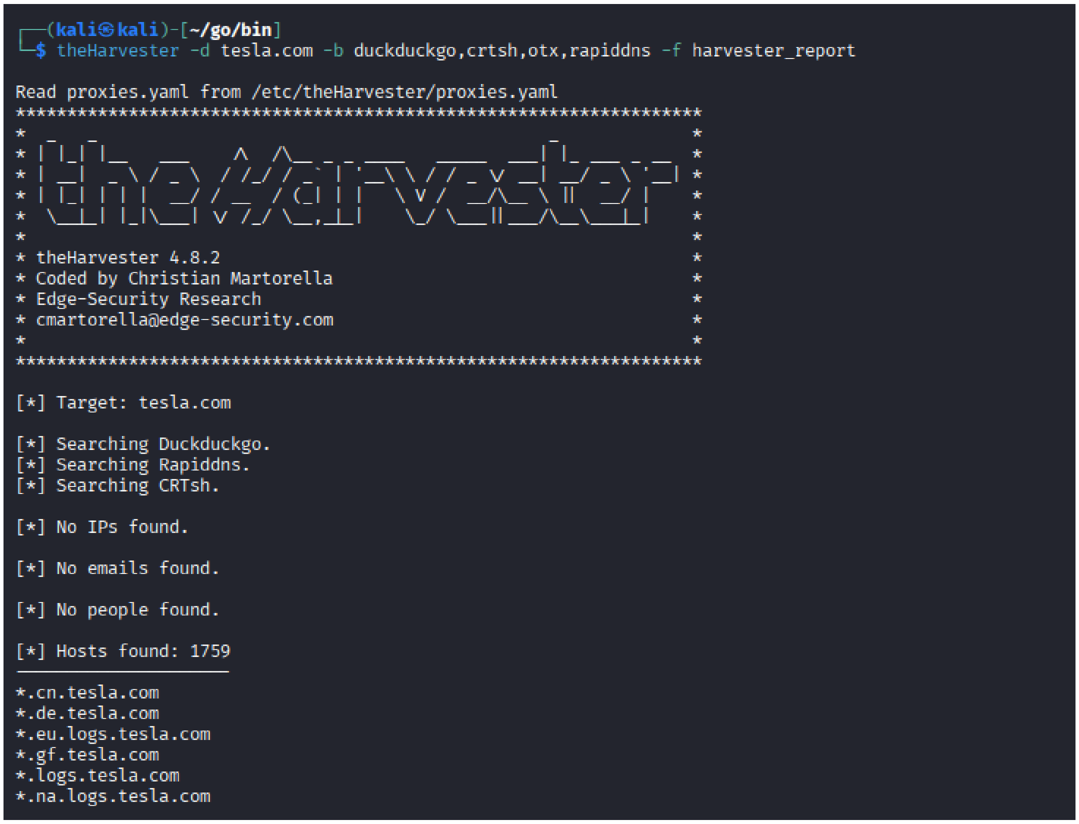
```
┌──(kali㉿kali)-[~/go/bin]
└─$ amass enum -passive -d example.com -o amass_subs.txt

[sudo] password for kali:
Checking for new libpostal data file...
New libpostal data file available
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
100 9951k  100 9951k    0     0  2765k      0  0:00:03  0:00:03 --:--:-- 3872k
address_expansions/
address_expansions/address_dictionary.dat
numex/
numex/numex.dat
transliteration/
transliteration/transliteration.dat
Checking for new libpostal parser data file...
New libpostal parser data file available
Downloading multipart: https://github.com/openvenues/libpostal/releases/download/v1.0.0/parser.tar.g
z, num_chunks=12
Downloading part 1: filename=/var/lib/libpostal/parser.tar.gz.1, offset=0, max=67108863
Downloading part 2: filename=/var/lib/libpostal/parser.tar.gz.2, offset=67108864, max=134217727
Downloading part 4: filename=/var/lib/libpostal/parser.tar.gz.4, offset=201326592, max=268435455
Downloading part 3: filename=/var/lib/libpostal/parser.tar.gz.3, offset=134217728, max=201326591
Downloading part 5: filename=/var/lib/libpostal/parser.tar.gz.5, offset=268435456, max=335544319
Downloading part 7: filename=/var/lib/libpostal/parser.tar.gz.7, offset=402653184, max=469762047
Downloading part 9: filename=/var/lib/libpostal/parser.tar.gz.9, offset=536870912, max=603979775
Downloading part 8: filename=/var/lib/libpostal/parser.tar.gz.8, offset=469762048, max=536870911
Downloading part 6: filename=/var/lib/libpostal/parser.tar.gz.6, offset=335544320, max=402653183
Downloading part 10: filename=/var/lib/libpostal/parser.tar.gz.10, offset=603979776, max=671088639
Downloading part 11: filename=/var/lib/libpostal/parser.tar.gz.11, offset=671088640, max=738197503
Downloading part 12: filename=/var/lib/libpostal/parser.tar.gz.12, offset=738197504, max=805306367
address_parser/
address_parser/address_parser_crf.dat
address_parser/address_parser_phrases.dat
address_parser/address_parser_postal_codes.dat
address_parser/address_parser_vocab.trie
```

Combine & sort:

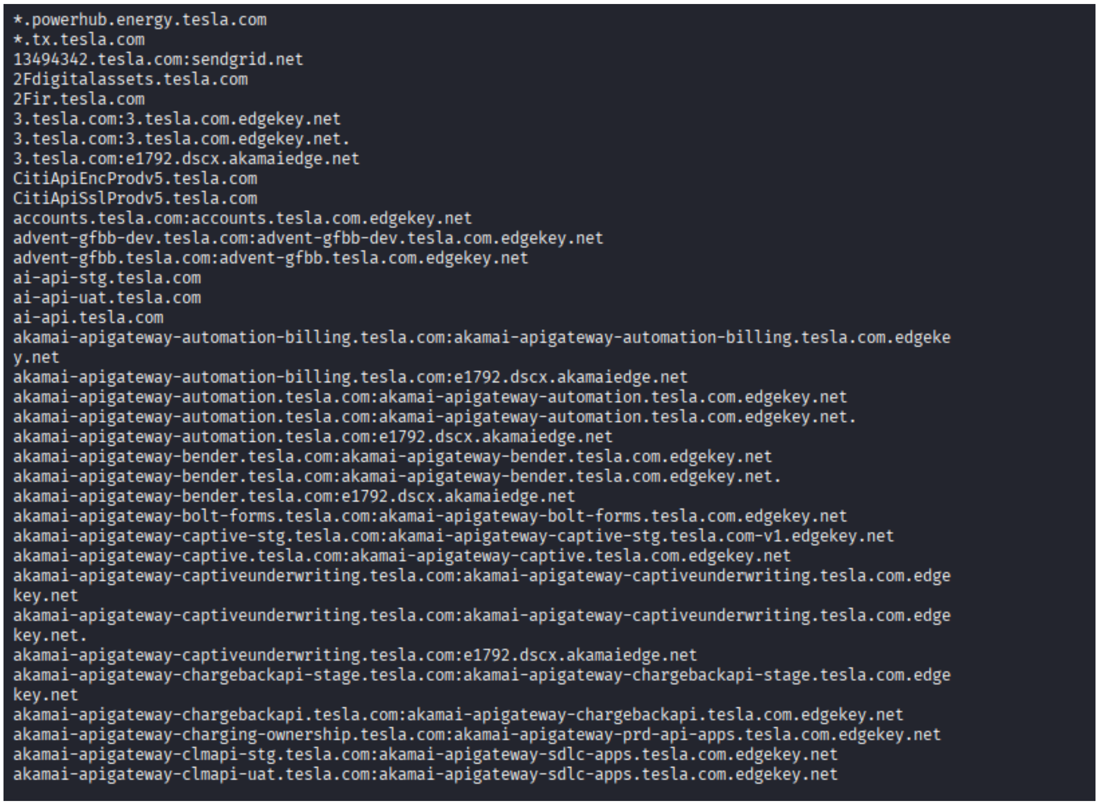
cat subdomains.txt amass_subs.txt | sort -u > final_subs.txt

STEP 3 — Email & Employee Information (theHarvester)

theHarvester -d example.com -b google,bing,linkedin -f harvester_report



```
┌──(kali㉿kali)-[~/go/bin]
└─$ theHarvester -d tesla.com -b duckduckgo,crtsh,otx,rapiddns -f harvester_report

Read proxies.yaml from /etc/theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.8.2                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: tesla.com

[*] Searching Duckduckgo.
[*] Searching Rapiddns.
[*] Searching CRTsh.

[*] No IPs found.

[*] No emails found.

[*] No people found.

[*] Hosts found: 1759
---------------------
*.cn.tesla.com
*.de.tesla.com
*.eu.logs.tesla.com
*.gf.tesla.com
*.logs.tesla.com
*.na.logs.tesla.com
```

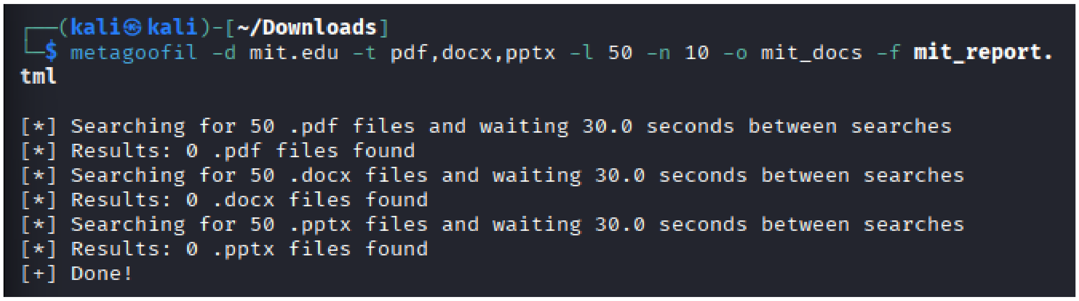


```
*.powerhub.energy.tesla.com
*.tx.tesla.com
13494342.tesla.com:sendgrid.net
2Fdigitalassets.tesla.com
2Fir.tesla.com
3.tesla.com:3.tesla.com.edgekey.net
3.tesla.com:3.tesla.com.edgekey.net.
3.tesla.com:e1792.dscx.akamaiedge.net
CitiApiEncProdv5.tesla.com
CitiApiSslProdv5.tesla.com
accounts.tesla.com:accounts.tesla.com.edgekey.net
advent-gfbb-dev.tesla.com:advent-gfbb-dev.tesla.com.edgekey.net
advent-gfbb.tesla.com:advent-gfbb.tesla.com.edgekey.net
ai-api-stg.tesla.com
ai-api-uat.tesla.com
ai-api.tesla.com
akamai-apigateway-automation-billing.tesla.com:akamai-apigateway-automation-billing.tesla.com.edgeke
y.net
akamai-apigateway-automation-billing.tesla.com:e1792.dscx.akamaiedge.net
akamai-apigateway-automation.tesla.com:akamai-apigateway-automation.tesla.com.edgekey.net
akamai-apigateway-automation.tesla.com:akamai-apigateway-automation.tesla.com.edgekey.net.
akamai-apigateway-automation.tesla.com:e1792.dscx.akamaiedge.net
akamai-apigateway-bender.tesla.com:akamai-apigateway-bender.tesla.com.edgekey.net
akamai-apigateway-bender.tesla.com:akamai-apigateway-bender.tesla.com.edgekey.net.
akamai-apigateway-bender.tesla.com:e1792.dscx.akamaiedge.net
akamai-apigateway-bolt-forms.tesla.com:akamai-apigateway-bolt-forms.tesla.com.edgekey.net
akamai-apigateway-captive-stg.tesla.com:akamai-apigateway-captive-stg.tesla.com-v1.edgekey.net
akamai-apigateway-captive.tesla.com:akamai-apigateway-captive.tesla.com.edgekey.net
akamai-apigateway-captiveunderwriting.tesla.com:akamai-apigateway-captiveunderwriting.tesla.com.edge
key.net
akamai-apigateway-captiveunderwriting.tesla.com:akamai-apigateway-captiveunderwriting.tesla.com.edge
key.net.
akamai-apigateway-captiveunderwriting.tesla.com:e1792.dscx.akamaiedge.net
akamai-apigateway-chargebackapi-stage.tesla.com:akamai-apigateway-chargebackapi-stage.tesla.com.edge
key.net
akamai-apigateway-chargebackapi.tesla.com:akamai-apigateway-chargebackapi.tesla.com.edgekey.net
akamai-apigateway-charging-ownership.tesla.com:akamai-apigateway-prd-api-apps.tesla.com.edgekey.net
akamai-apigateway-clmapi-stg.tesla.com:akamai-apigateway-sdlc-apps.tesla.com.edgekey.net
akamai-apigateway-clmapi-uat.tesla.com:akamai-apigateway-sdlc-apps.tesla.com.edgekey.net
```

STEP 4 — Metadata Extraction

1. Search & Download Public Files Using metagoofil

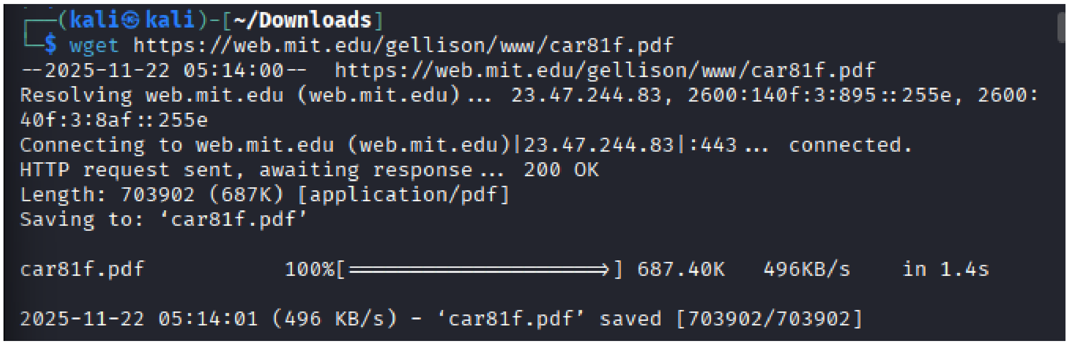
metagoofil -d mit.edu -t pdf,doc,docx,pptx -l 100 -n 10 -o downloads -f meta_report.html



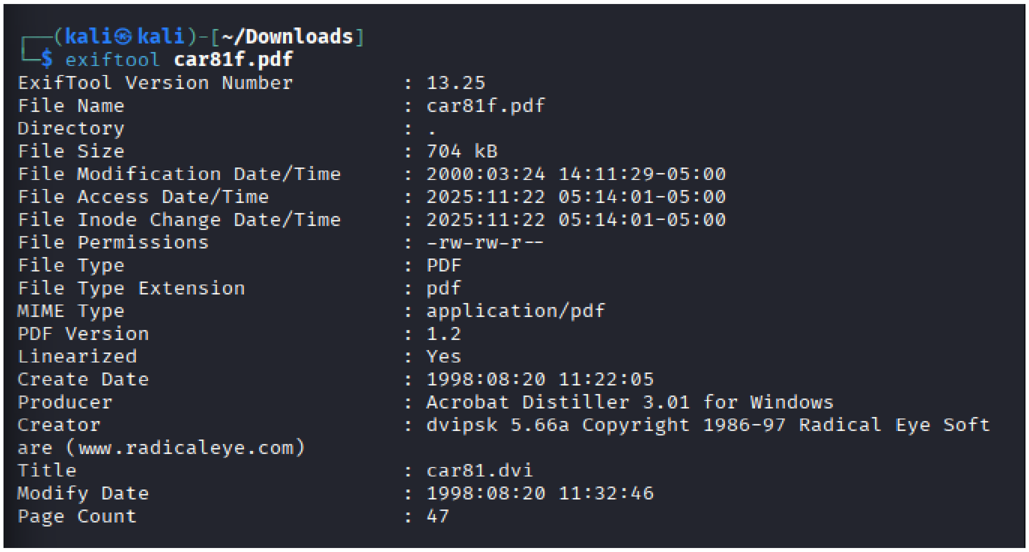
```
┌──(kali㉿kali)-[~/Downloads]
└─$ metagoofil -d mit.edu -t pdf,docx,pptx -l 50 -n 10 -o mit_docs -f mit_report.
tml

[*] Searching for 50 .pdf files and waiting 30.0 seconds between searches
[*] Results: 0 .pdf files found
[*] Searching for 50 .docx files and waiting 30.0 seconds between searches
[*] Results: 0 .docx files found
[*] Searching for 50 .pptx files and waiting 30.0 seconds between searches
[*] Results: 0 .pptx files found
[+] Done!
```

2. Extract Metadata Using exiftool

exiftool file.pdf



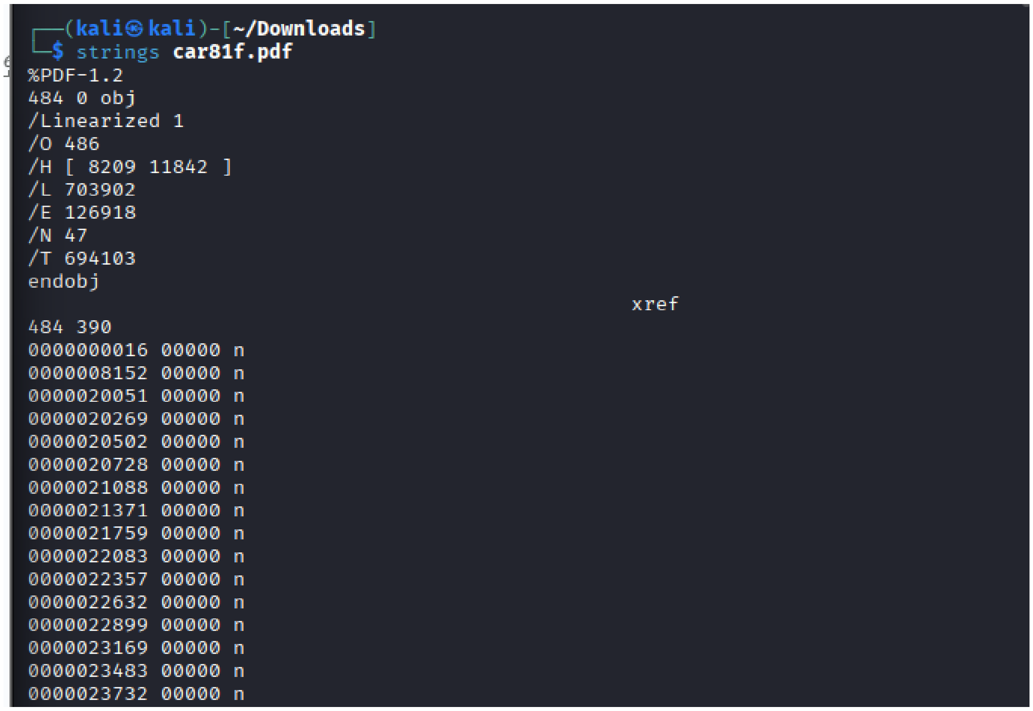
```
┌──(kali㉿kali)-[~/Downloads]
└─$ wget https://web.mit.edu/gellison/www/car81f.pdf
--2025-11-22 05:14:00--  https://web.mit.edu/gellison/www/car81f.pdf
Resolving web.mit.edu (web.mit.edu)... 23.47.244.83, 2600:140f:3:895::255e, 2600:
40f:3:8af::255e
Connecting to web.mit.edu (web.mit.edu)|23.47.244.83|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 703902 (687K) [application/pdf]
Saving to: ‘car81f.pdf’

car81f.pdf          100%[====================>] 687.40K   496KB/s    in 1.4s

2025-11-22 05:14:01 (496 KB/s) - ‘car81f.pdf’ saved [703902/703902]
```



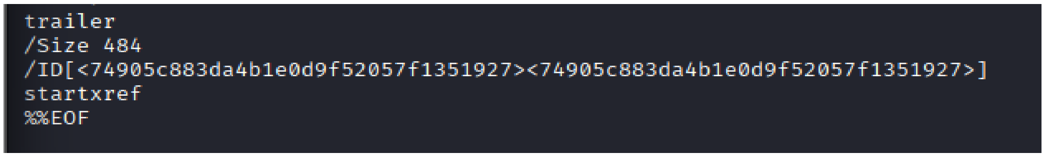
```
┌──(kali㉿kali)-[~/Downloads]
└─$ exiftool car81f.pdf
ExifTool Version Number         : 13.25
File Name                       : car81f.pdf
Directory                       : .
File Size                       : 704 kB
File Modification Date/Time     : 2000:03:24 14:11:29-05:00
File Access Date/Time           : 2025:11:22 05:14:01-05:00
File Inode Change Date/Time     : 2025:11:22 05:14:01-05:00
File Permissions                : -rw-rw-r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.2
Linearized                      : Yes
Create Date                     : 1998:08:20 11:22:05
Producer                        : Acrobat Distiller 3.01 for Windows
Creator                         : dvipsk 5.66a Copyright 1986-97 Radical Eye Soft
are (www.radicaleye.com)
Title                           : car81.dvi
Modify Date                     : 1998:08:20 11:32:46
Page Count                      : 47
```

3. strings

strings file.pdf | head



```
┌──(kali㉿kali)-[~/Downloads]
└─$ strings car81f.pdf
%PDF-1.2
484 0 obj
/Linearized 1
/O 486
/H [ 8209 11842 ]
/L 703902
/E 126918
/N 47
/T 694103
endobj
                                                  xref
484 390
0000000016 00000 n
0000008152 00000 n
0000020051 00000 n
0000020269 00000 n
0000020502 00000 n
0000020728 00000 n
0000021088 00000 n
0000021371 00000 n
0000021759 00000 n
0000022083 00000 n
0000022357 00000 n
0000022632 00000 n
0000022899 00000 n
0000023169 00000 n
0000023483 00000 n
0000023732 00000 n
```

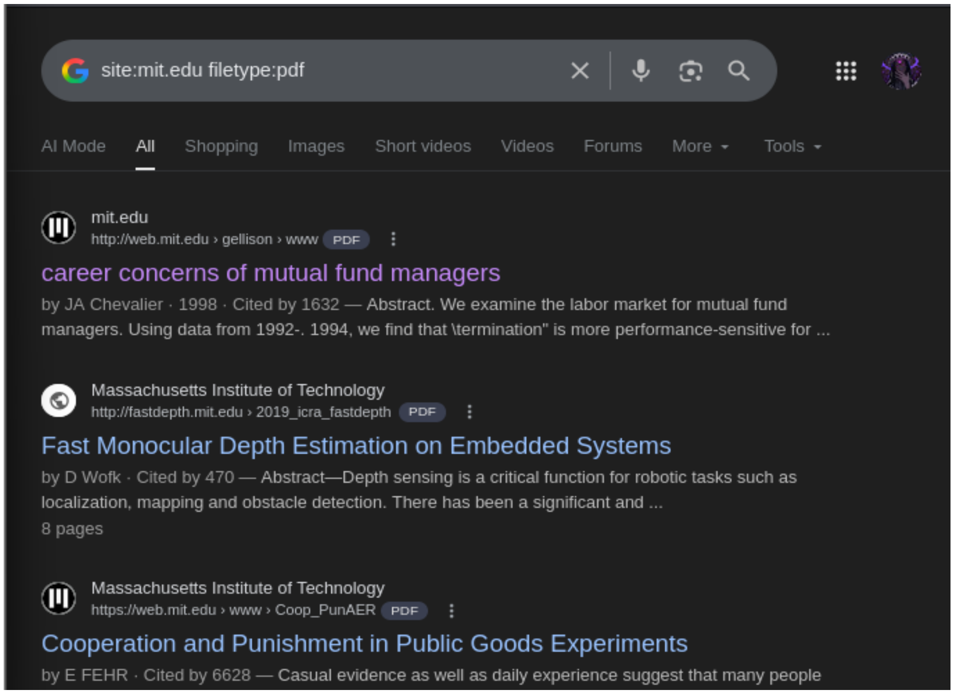


```
trailer
/Size 484
/ID[<74905c883da4b1e0d9f52057f1351927><74905c883da4b1e0d9f52057f1351927>]
startxref
%%EOF
```

STEP 5 — Google Dorking (Passive OSINT)

Examples:

site:example.com filetype:pdf
site:example.com intitle:"index of"
site:example.com inurl:admin
site:example.com ext:log
site:example.com "password"
site:example.com "confidential".



site:mit.edu filetype:pdf

mit.edu
http://web.mit.edu › gellison › www PDF

career concerns of mutual fund managers

by JA Chevalier · 1998 · Cited by 1632 — Abstract. We examine the labor market for mutual fund managers. Using data from 1992-. 1994, we find that \termination" is more performance-sensitive for ...

Massachusetts Institute of Technology
http://fastdepth.mit.edu › 2019_icra_fastdepth PDF

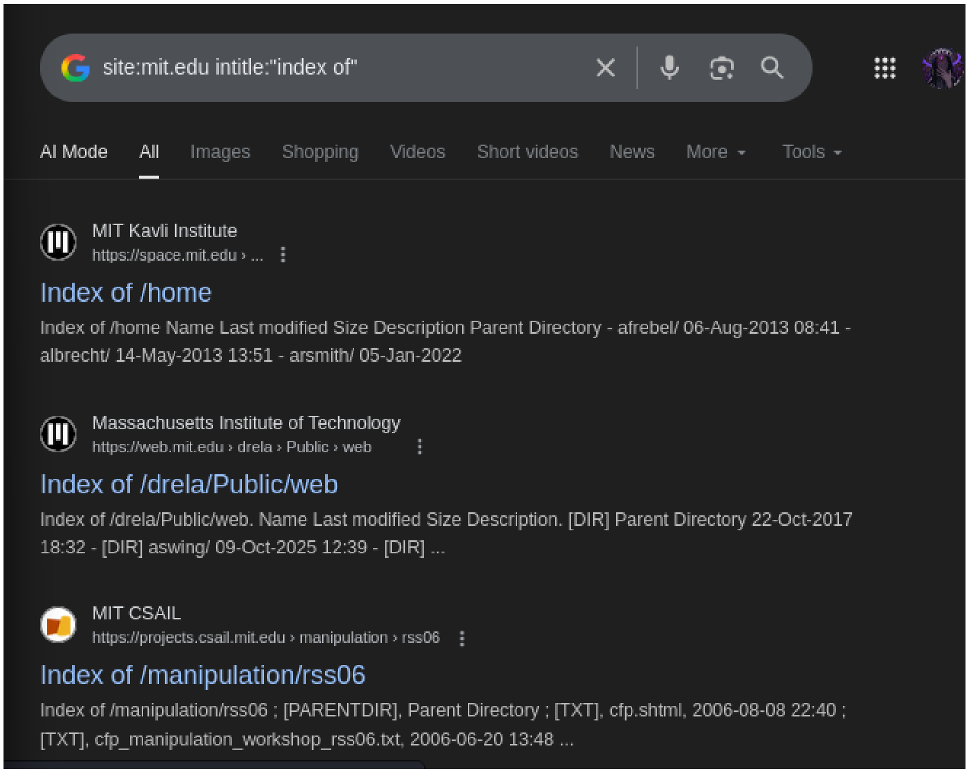
Fast Monocular Depth Estimation on Embedded Systems

by D Wofk · Cited by 470 — Abstract—Depth sensing is a critical function for robotic tasks such as localization, mapping and obstacle detection. There has been a significant and ...
8 pages

Massachusetts Institute of Technology
https://web.mit.edu › www › Coop_PunAER PDF

Cooperation and Punishment in Public Goods Experiments

by E FEHR · Cited by 6628 — Casual evidence as well as daily experience suggest that many people



site:mit.edu intitle:"index of"

MIT Kavli Institute
https://space.mit.edu › ...

Index of /home

Index of /home Name Last modified Size Description Parent Directory - afrebel/ 06-Aug-2013 08:41 - albrecht/ 14-May-2013 13:51 - arsmith/ 05-Jan-2022

Massachusetts Institute of Technology
https://web.mit.edu › drela › Public › web

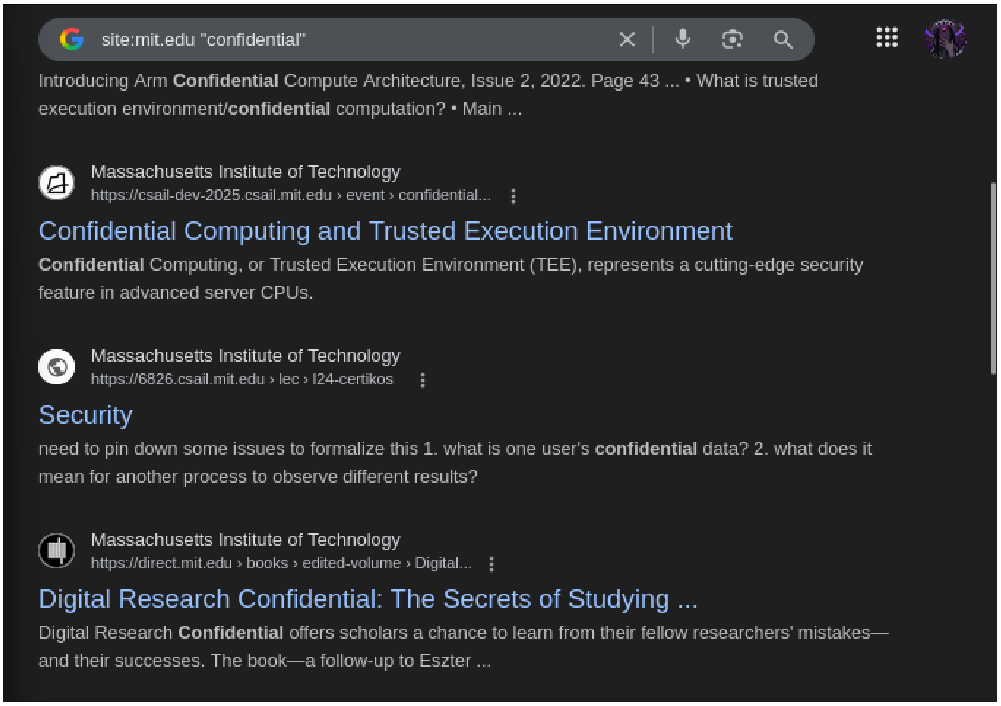
Index of /drela/Public/web

Index of /drela/Public/web. Name Last modified Size Description. [DIR] Parent Directory 22-Oct-2017 18:32 - [DIR] aswing/ 09-Oct-2025 12:39 - [DIR] ...

MIT CSAIL
https://projects.csail.mit.edu › manipulation › rss06

Index of /manipulation/rss06

Index of /manipulation/rss06 ; [PARENTDIR], Parent Directory ; [TXT], cfp.shtml, 2006-08-08 22:40 ; [TXT], cfp_manipulation_workshop_rss06.txt, 2006-06-20 13:48 ...



site:mit.edu "confidential"

Introducing Arm **Confidential** Compute Architecture, Issue 2, 2022. Page 43 ... • What is trusted execution environment/**confidential** computation? • Main ...

Massachusetts Institute of Technology
https://csail-dev-2025.csail.mit.edu › event › confidential...

Confidential Computing and Trusted Execution Environment

Confidential Computing, or Trusted Execution Environment (TEE), represents a cutting-edge security feature in advanced server CPUs.

Massachusetts Institute of Technology
https://6826.csail.mit.edu › lec › l24-certikos

Security

need to pin down some issues to formalize this 1. what is one user's **confidential** data? 2. what does it mean for another process to observe different results?

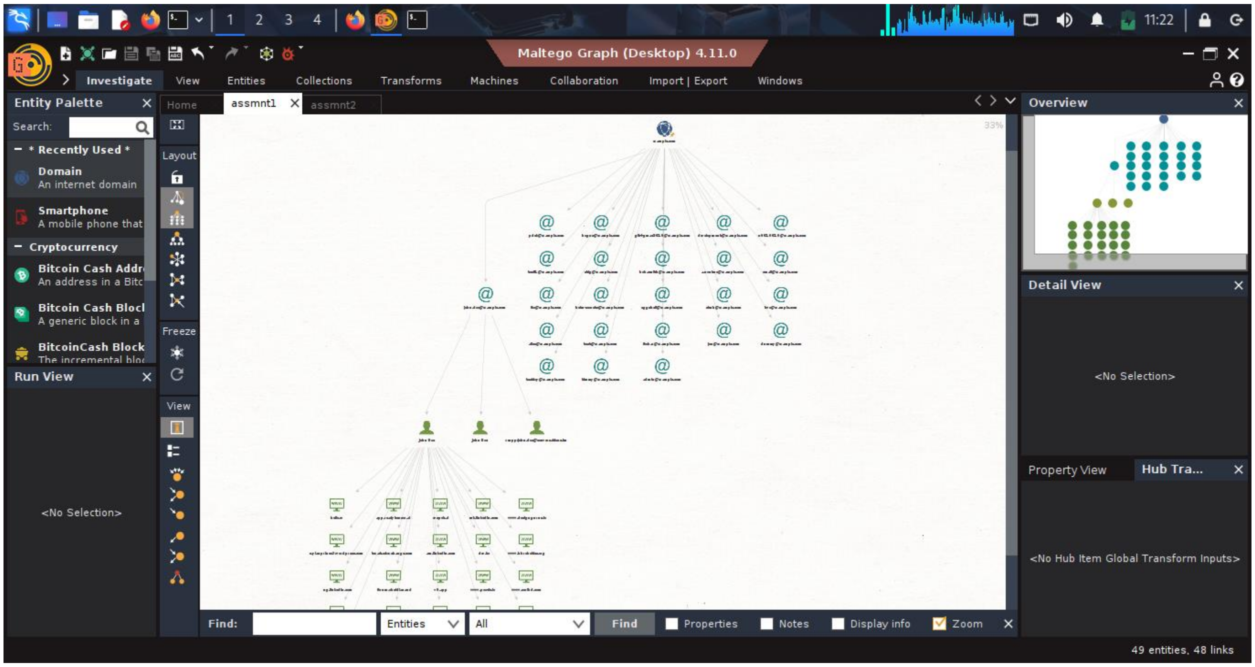
Massachusetts Institute of Technology
https://direct.mit.edu › books › edited-volume › Digital...

Digital Research Confidential: The Secrets of Studying ...

Digital Research **Confidential** offers scholars a chance to learn from their fellow researchers' mistakes—and their successes. The book—a follow-up to Eszter ...

STEP 6 — Social Media & OSINT (Maltego / SpiderFoot)

Using Maltego (CE):



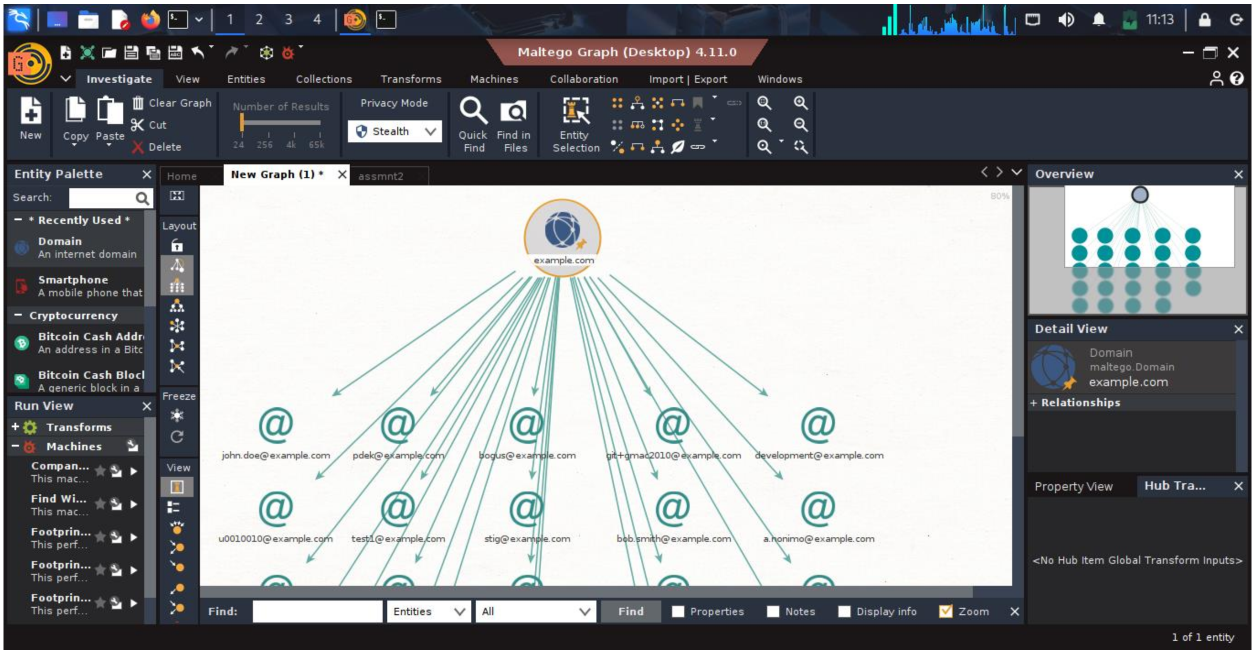
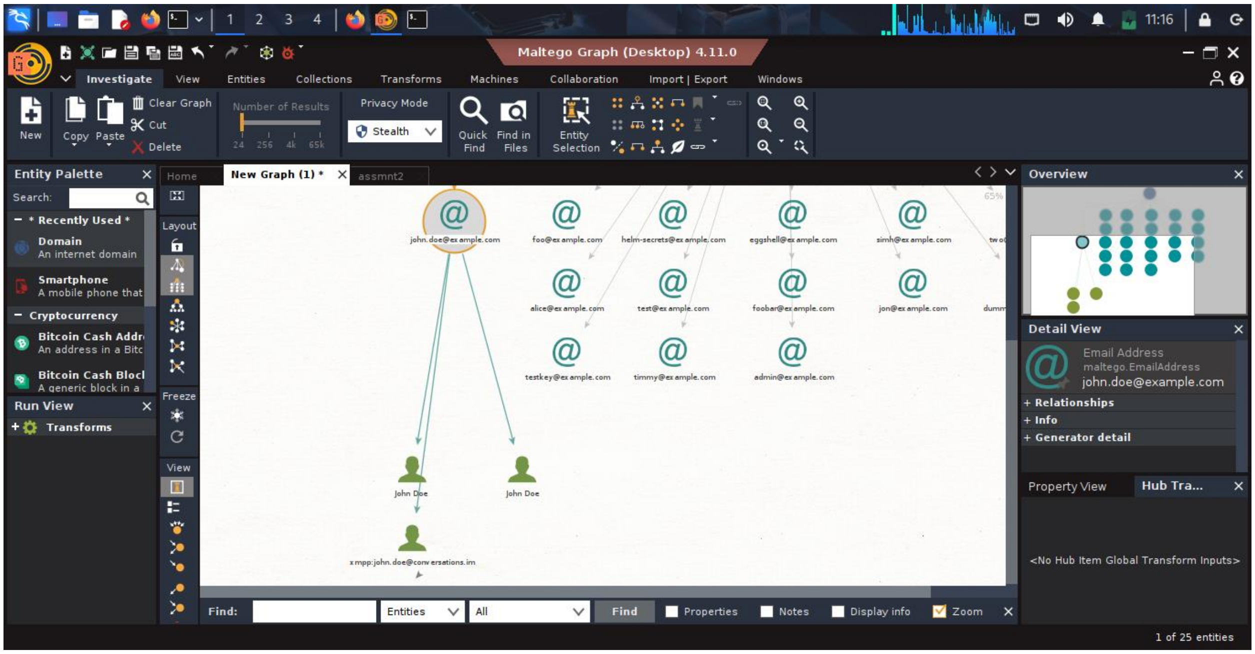
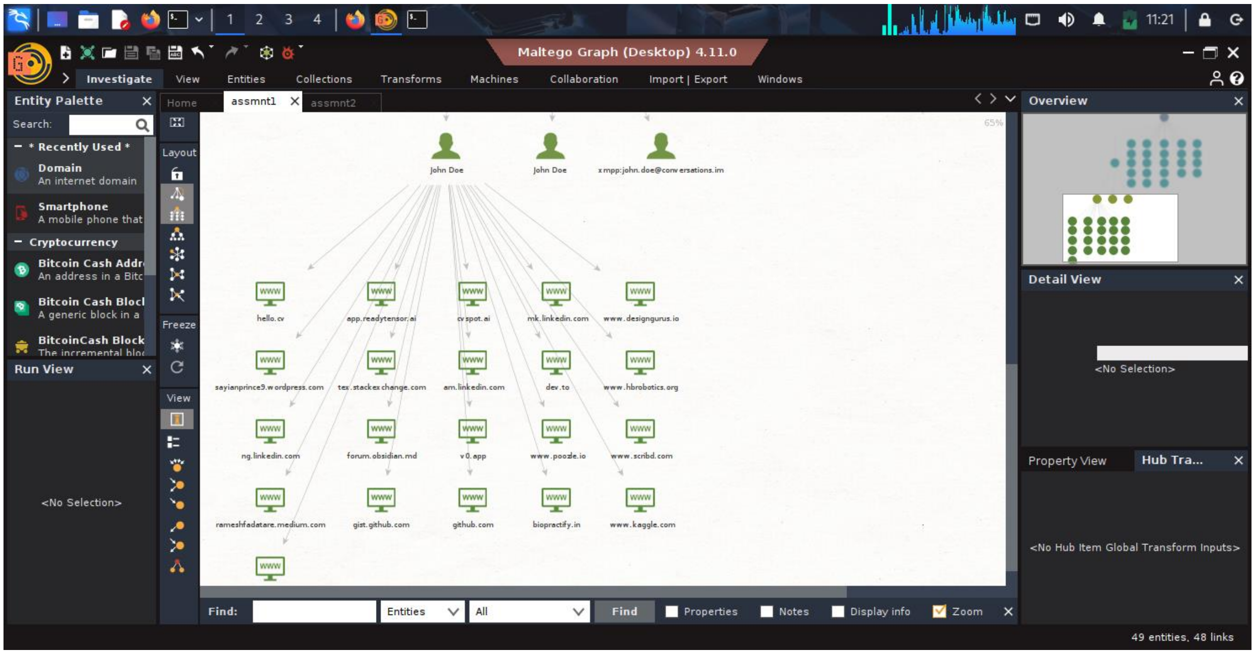


Figure: set Domain as example.com



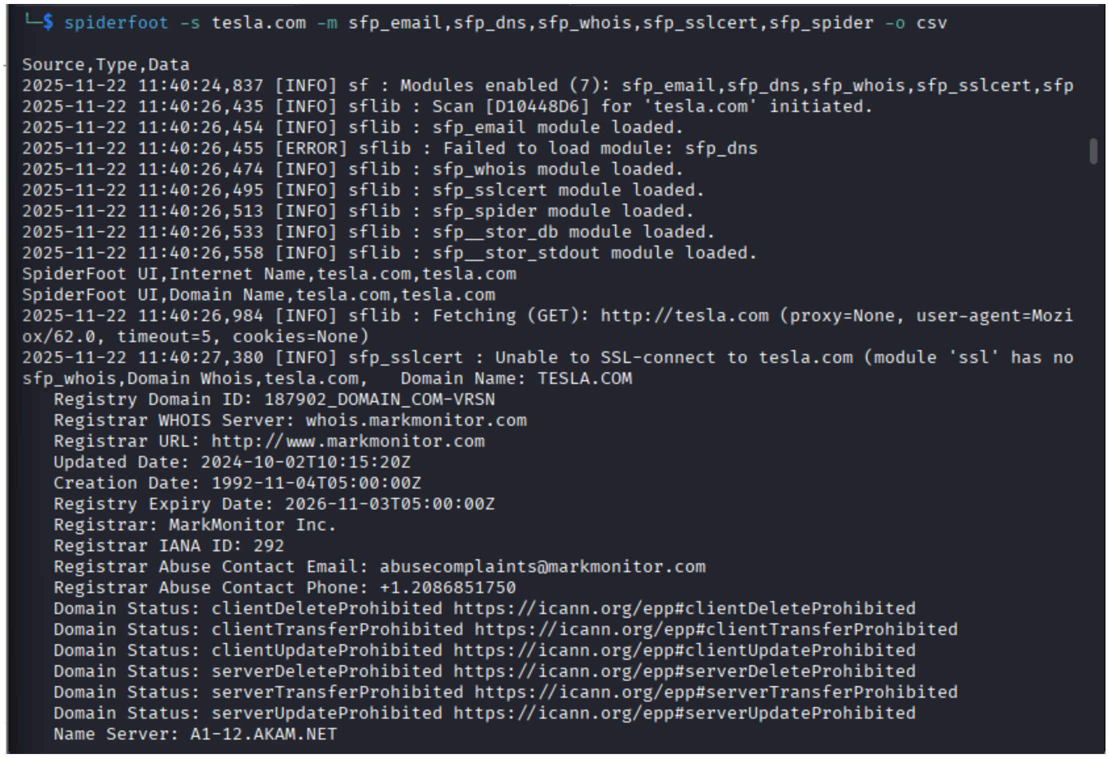
Found people from email



user related links-github,linedin etc

1.Using SpiderFoot:

spiderfoot -s tesla.com -m sfp_email,sfp_dns,sfp_whois,sfp_sslcert,sfp_spider -o csv



```
└─$ spiderfoot -s tesla.com -m sfp_email,sfp_dns,sfp_whois,sfp_sslcert,sfp_spider -o csv

Source,Type,Data
2025-11-22 11:40:24,837 [INFO] sf : Modules enabled (7): sfp_email,sfp_dns,sfp_whois,sfp_sslcert,sfp
2025-11-22 11:40:26,435 [INFO] sflib : Scan [D10448D6] for 'tesla.com' initiated.
2025-11-22 11:40:26,454 [INFO] sflib : sfp_email module loaded.
2025-11-22 11:40:26,455 [ERROR] sflib : Failed to load module: sfp_dns
2025-11-22 11:40:26,474 [INFO] sflib : sfp_whois module loaded.
2025-11-22 11:40:26,495 [INFO] sflib : sfp_sslcert module loaded.
2025-11-22 11:40:26,513 [INFO] sflib : sfp_spider module loaded.
2025-11-22 11:40:26,533 [INFO] sflib : sfp__stor_db module loaded.
2025-11-22 11:40:26,558 [INFO] sflib : sfp__stor_stdout module loaded.
SpiderFoot UI,Internet Name,tesla.com,tesla.com
SpiderFoot UI,Domain Name,tesla.com,tesla.com
2025-11-22 11:40:26,984 [INFO] sflib : Fetching (GET): http://tesla.com (proxy=None, user-agent=Mozi
ox/62.0, timeout=5, cookies=None)
2025-11-22 11:40:27,380 [INFO] sfp_sslcert : Unable to SSL-connect to tesla.com (module 'ssl' has no
sfp_whois,Domain Whois,tesla.com,   Domain Name: TESLA.COM
   Registry Domain ID: 187902_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2024-10-02T10:15:20Z
   Creation Date: 1992-11-04T05:00:00Z
   Registry Expiry Date: 2026-11-03T05:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: A1-12.AKAM.NET
```

Domain WHOIS information

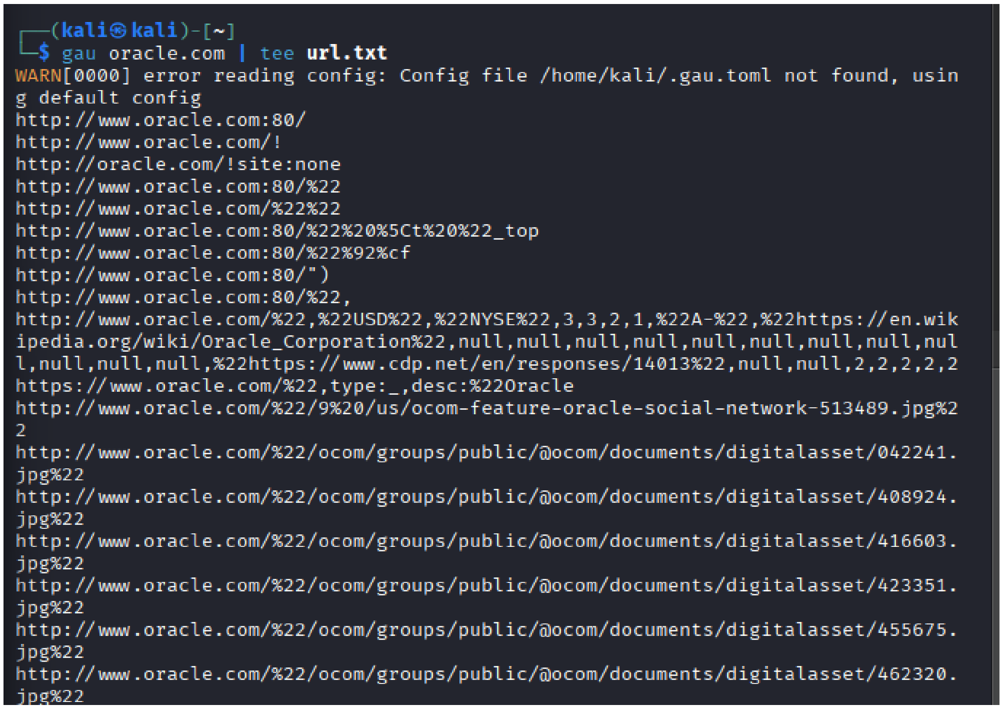
output (registrar, creation date, expiry date, registrant org), including:

- **Registrant Organization**: DNStination Inc.
- **Registrar**: MarkMonitor
- **Created**: 1992
- **Expires**: 2026
- **Name servers**: Akamai + UltraDNS
- **Admin contact email**: admin@dnstinations.com → This is real OSINT.

STEP 7 — Collect All URLs

1. GAU

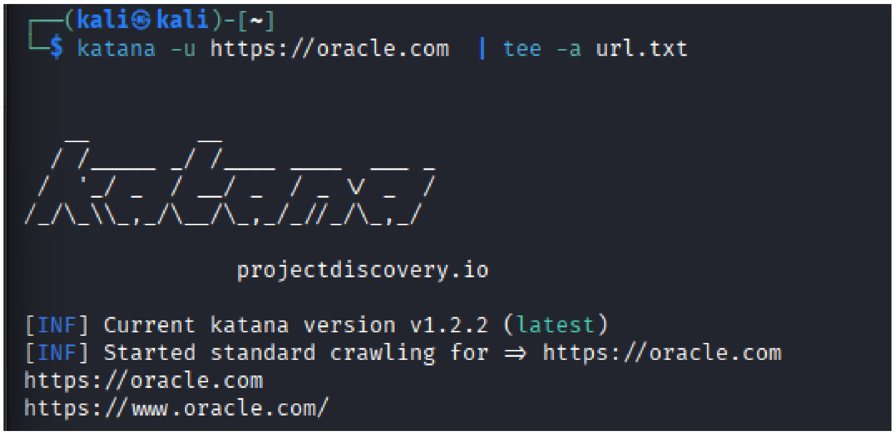
gau oracle.com | tee url.txt



```
┌──(kali㉿kali)-[~]
└─$ gau oracle.com | tee url.txt
WARN[0000] error reading config: Config file /home/kali/.gau.toml not found, usin
g default config
http://www.oracle.com:80/
http://www.oracle.com/!
http://oracle.com/!site:none
http://www.oracle.com:80/%22
http://www.oracle.com/%22%22
http://www.oracle.com:80/%22%20%5Ct%20%22_top
http://www.oracle.com:80/%22%92%cf
http://www.oracle.com:80/")
http://www.oracle.com:80/%22,
http://www.oracle.com/%22,%22USD%22,%22NYSE%22,3,3,2,1,%22A-%22,%22https://en.wik
ipedia.org/wiki/Oracle_Corporation%22,null,null,null,null,null,null,null,null,nul
l,null,null,null,%22https://www.cdp.net/en/responses/14013%22,null,null,2,2,2,2,2
https://www.oracle.com/%22,type:_,desc:%22Oracle
http://www.oracle.com/%22/9%20/us/ocom-feature-oracle-social-network-513489.jpg%2
2
http://www.oracle.com/%22/ocom/groups/public/@ocom/documents/digitalasset/042241.
jpg%22
http://www.oracle.com/%22/ocom/groups/public/@ocom/documents/digitalasset/408924.
jpg%22
http://www.oracle.com/%22/ocom/groups/public/@ocom/documents/digitalasset/416603.
jpg%22
http://www.oracle.com/%22/ocom/groups/public/@ocom/documents/digitalasset/423351.
jpg%22
http://www.oracle.com/%22/ocom/groups/public/@ocom/documents/digitalasset/455675.
jpg%22
http://www.oracle.com/%22/ocom/groups/public/@ocom/documents/digitalasset/462320.
jpg%22
```

2. katana

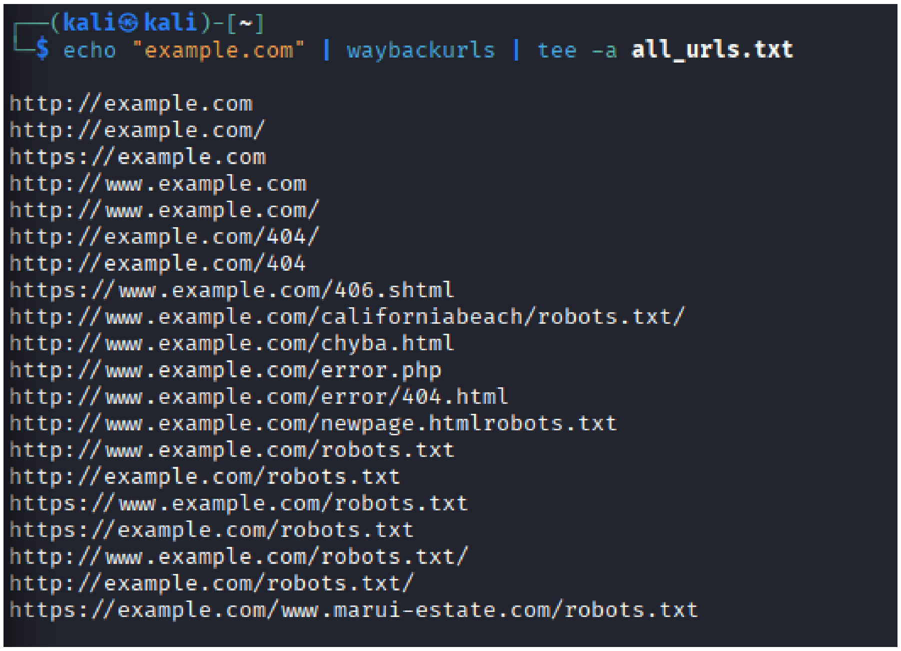
katana -u https://oracle.com | tee -a urls.txt



```
┌──(kali㉿kali)-[~]
└─$ katana -u https://oracle.com  | tee -a url.txt


   __        __
  / /_____ _/ /____ ____  ___ _
 /  '_/ _  / __/ _  / _ \/ _  /
/_/\_\\_,_/\__/\_,_/_//_/\_,_/

                projectdiscovery.io

[INF] Current katana version v1.2.2 (latest)
[INF] Started standard crawling for => https://oracle.com
https://oracle.com
https://www.oracle.com/
```

3. waybackurl

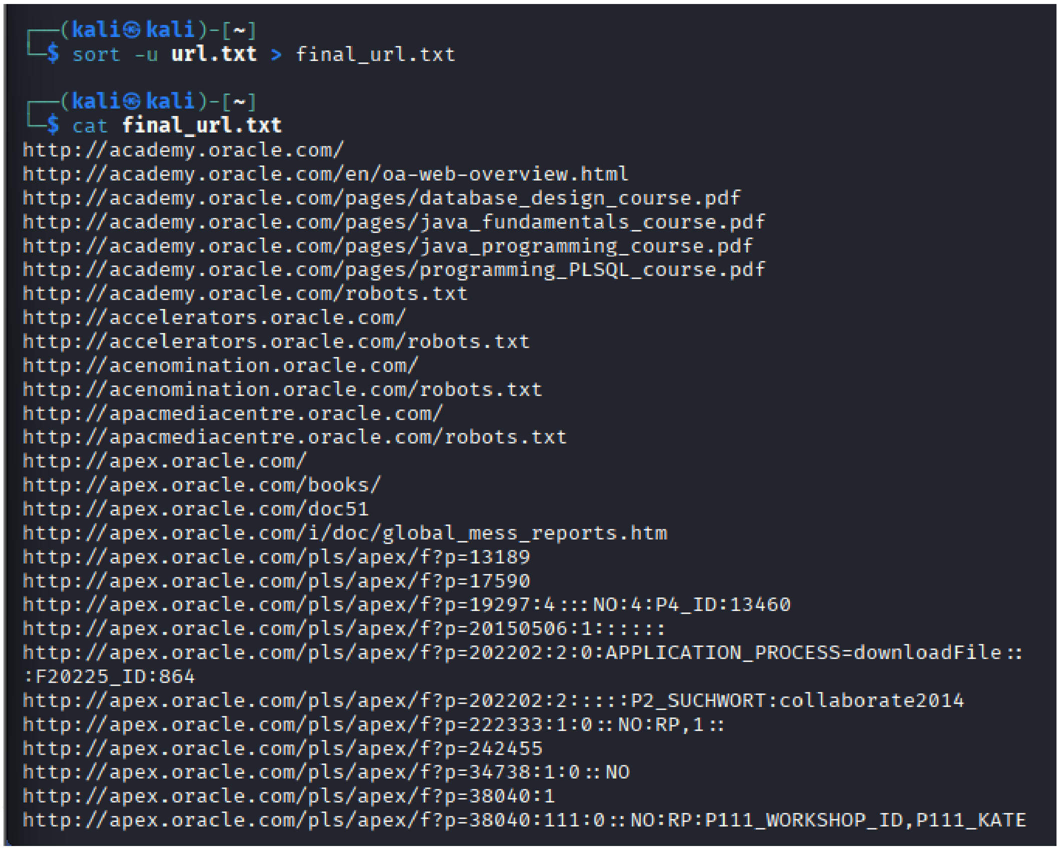
waybackurls example.com >> urls.txt



```
┌──(kali㉿kali)-[~]
└─$ echo "example.com" | waybackurls | tee -a all_urls.txt

http://example.com
http://example.com/
https://example.com
http://www.example.com
http://www.example.com/
http://example.com/404/
http://example.com/404
https://www.example.com/406.shtml
http://www.example.com/californiabeach/robots.txt/
http://www.example.com/chyba.html
http://www.example.com/error.php
http://www.example.com/error/404.html
http://www.example.com/newpage.htmlrobots.txt
http://www.example.com/robots.txt
http://example.com/robots.txt
https://www.example.com/robots.txt
https://example.com/robots.txt
http://www.example.com/robots.txt/
http://example.com/robots.txt/
https://example.com/www.marui-estate.com/robots.txt
```

Filter unique URLs:

sort -u urls.txt > final_urls.txt

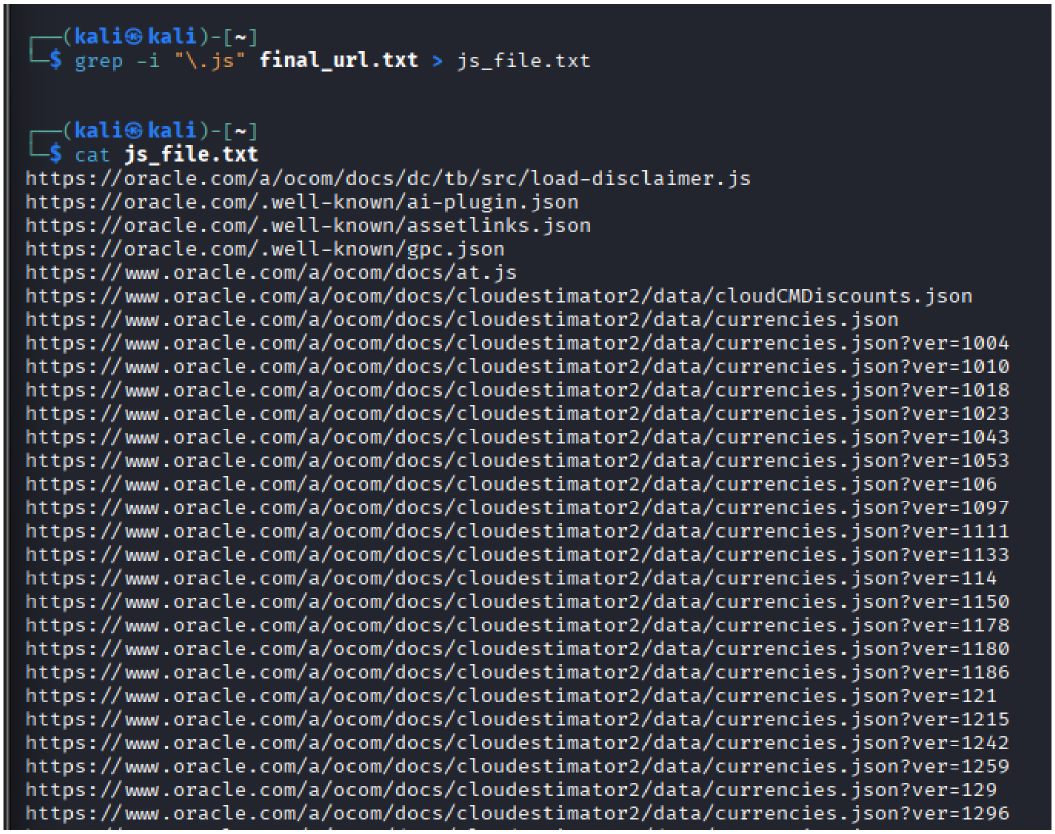


```
┌──(kali㉿kali)-[~]
└─$ sort -u url.txt > final_url.txt

┌──(kali㉿kali)-[~]
└─$ cat final_url.txt
http://academy.oracle.com/
http://academy.oracle.com/en/oa-web-overview.html
http://academy.oracle.com/pages/database_design_course.pdf
http://academy.oracle.com/pages/java_fundamentals_course.pdf
http://academy.oracle.com/pages/java_programming_course.pdf
http://academy.oracle.com/pages/programming_PLSQL_course.pdf
http://academy.oracle.com/robots.txt
http://accelerators.oracle.com/
http://accelerators.oracle.com/robots.txt
http://acenomination.oracle.com/
http://acenomination.oracle.com/robots.txt
http://apacmediacentre.oracle.com/
http://apacmediacentre.oracle.com/robots.txt
http://apex.oracle.com/
http://apex.oracle.com/books/
http://apex.oracle.com/doc51
http://apex.oracle.com/i/doc/global_mess_reports.htm
http://apex.oracle.com/pls/apex/f?p=13189
http://apex.oracle.com/pls/apex/f?p=17590
http://apex.oracle.com/pls/apex/f?p=19297:4:::NO:4:P4_ID:13460
http://apex.oracle.com/pls/apex/f?p=20150506:1::::::
http://apex.oracle.com/pls/apex/f?p=202202:2:0:APPLICATION_PROCESS=downloadFile::
:F20225_ID:864
http://apex.oracle.com/pls/apex/f?p=202202:2::::P2_SUCHWORT:collaborate2014
http://apex.oracle.com/pls/apex/f?p=222333:1:0::NO:RP,1::
http://apex.oracle.com/pls/apex/f?p=242455
http://apex.oracle.com/pls/apex/f?p=34738:1:0::NO
http://apex.oracle.com/pls/apex/f?p=38040:1
http://apex.oracle.com/pls/apex/f?p=38040:111:0::NO:RP:P111_WORKSHOP_ID,P111_KATE
```

STEP 8 — Extract JS Files

1. Extract JS URLs

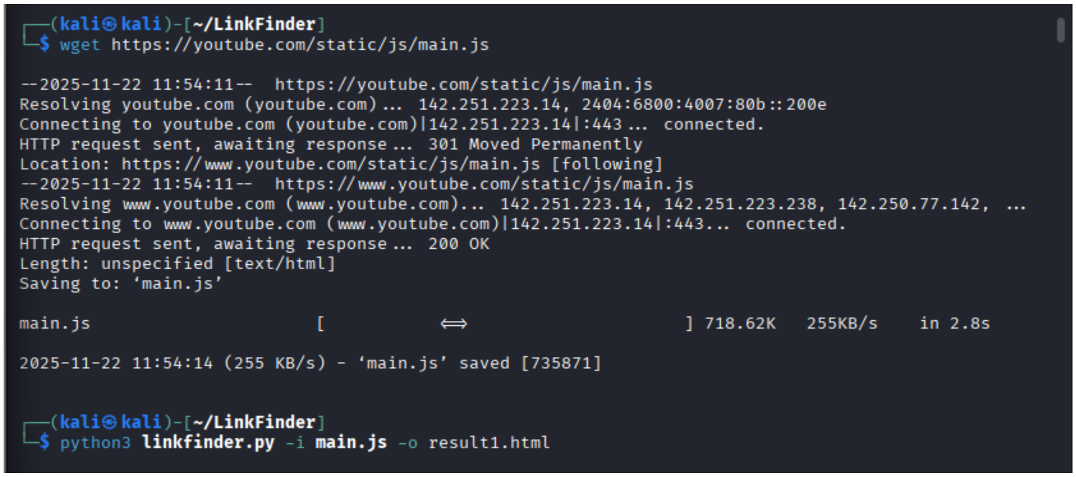
cat final_urls.txt | grep "\.js$" > js_files.txt



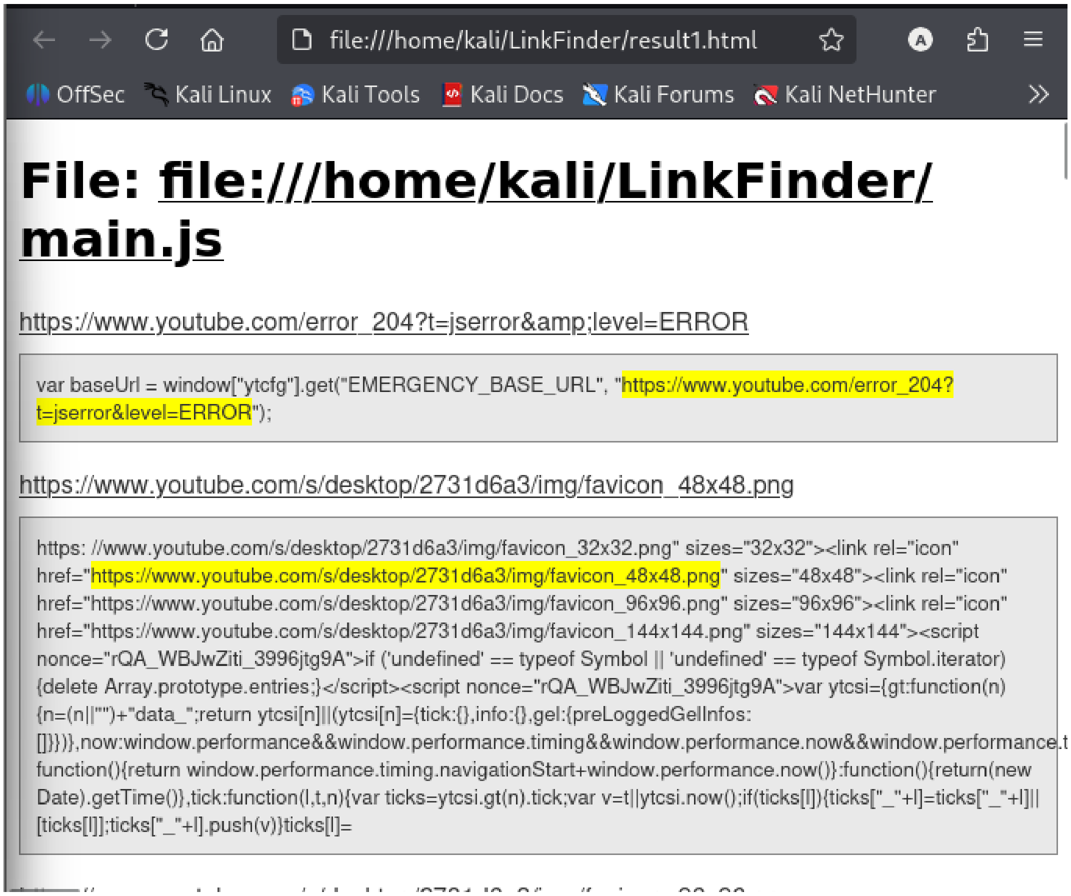
```
┌──(kali㉿kali)-[~]
└─$ grep -i "\.js" final_url.txt > js_file.txt


┌──(kali㉿kali)-[~]
└─$ cat js_file.txt
https://oracle.com/a/ocom/docs/dc/tb/src/load-disclaimer.js
https://oracle.com/.well-known/ai-plugin.json
https://oracle.com/.well-known/assetlinks.json
https://oracle.com/.well-known/gpc.json
https://www.oracle.com/a/ocom/docs/at.js
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/cloudCMDiscounts.json
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=1004
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=1010
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=1018
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=1023
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=1043
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=1053
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=106
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=1097
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=1111
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=1133
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=114
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=1150
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=1178
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=1180
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=1186
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=121
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=1215
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=1242
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=1259
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=129
https://www.oracle.com/a/ocom/docs/cloudestimator2/data/currencies.json?ver=1296
```

2. Find JS Endpoints (LinkFinder)

python3 linkfinder.py -i js_files.txt -o results.html



```
┌──(kali㉿kali)-[~/LinkFinder]
└─$ wget https://youtube.com/static/js/main.js

--2025-11-22 11:54:11--  https://youtube.com/static/js/main.js
Resolving youtube.com (youtube.com)... 142.251.223.14, 2404:6800:4007:80b::200e
Connecting to youtube.com (youtube.com)|142.251.223.14|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.youtube.com/static/js/main.js [following]
--2025-11-22 11:54:11--  https://www.youtube.com/static/js/main.js
Resolving www.youtube.com (www.youtube.com)... 142.251.223.14, 142.251.223.238, 142.250.77.142, ...
Connecting to www.youtube.com (www.youtube.com)|142.251.223.14|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘main.js’

main.js                      [          <=>                    ] 718.62K   255KB/s    in 2.8s

2025-11-22 11:54:14 (255 KB/s) - ‘main.js’ saved [735871]


┌──(kali㉿kali)-[~/LinkFinder]
└─$ python3 linkfinder.py -i main.js -o result1.html
```



File: file:///home/kali/LinkFinder/main.js

https://www.youtube.com/error_204?t=jserror&amp;level=ERROR

```
var baseUrl = window["ytcfg"].get("EMERGENCY_BASE_URL", "https://www.youtube.com/error_204?
t=jserror&level=ERROR");
```

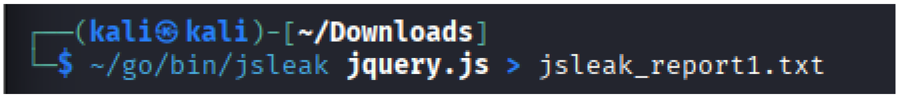
https://www.youtube.com/s/desktop/2731d6a3/img/favicon_48x48.png

```
https: //www.youtube.com/s/desktop/2731d6a3/img/favicon_32x32.png" sizes="32x32"><link rel="icon"
href="https://www.youtube.com/s/desktop/2731d6a3/img/favicon_48x48.png" sizes="48x48"><link rel="icon"
href="https://www.youtube.com/s/desktop/2731d6a3/img/favicon_96x96.png" sizes="96x96"><link rel="icon"
href="https://www.youtube.com/s/desktop/2731d6a3/img/favicon_144x144.png" sizes="144x144"><script
nonce="rQA_WBJwZiti_3996jtg9A">if ('undefined' == typeof Symbol || 'undefined' == typeof Symbol.iterator)
{delete Array.prototype.entries;}</script><script nonce="rQA_WBJwZiti_3996jtg9A">var ytcsi={gt:function(n)
{n=(n||"")+"data_";return ytcsi[n]||(ytcsi[n]={tick:{},info:{},gel:{preLoggedGelInfos:
[]}})},now:window.performance&&window.performance.timing&&window.performance.now&&window.performance.t
function(){return window.performance.timing.navigationStart+window.performance.now()}:function(){return(new
Date).getTime()},tick:function(l,t,n){var ticks=ytcsi.gt(n).tick;var v=t||ytcsi.now();if(ticks[l]){ticks["_"+l]=ticks["_"+l]||
[ticks[l]];ticks["_"+l].push(v)}ticks[l]=
```

LinkFinder successfully extracted multiple URLs from the JavaScript file.
All detected endpoints were publicly accessible static files.
No sensitive or internal endpoints were exposed in the JavaScript.

3. Find Secrets in JS (JSleak)

jsleak -url https://example.com -output jsleak_report.txt



```
┌──(kali㉿kali)-[~/Downloads]
└─$ ~/go/bin/jsleak jquery.js > jsleak_report1.txt
```

JS leak can reveal:

- API keys
- Tokens
- Endpoints
- Hardcoded credentials

9. Conclusion

Possible Attack Surfaces Identified:

- Misconfigured DNS entries
- Sensitive metadata inside documents
- Exposed JS files containing endpoints or configuration
- Public email addresses
  Identified subdomains (potentially