INFORMATION GATHERING

Introduction:

This report provides an overview of the information gathered about the website (https://google-gruyere.appspot.com/) using advanced Google search techniques, Shodan, and Censys.

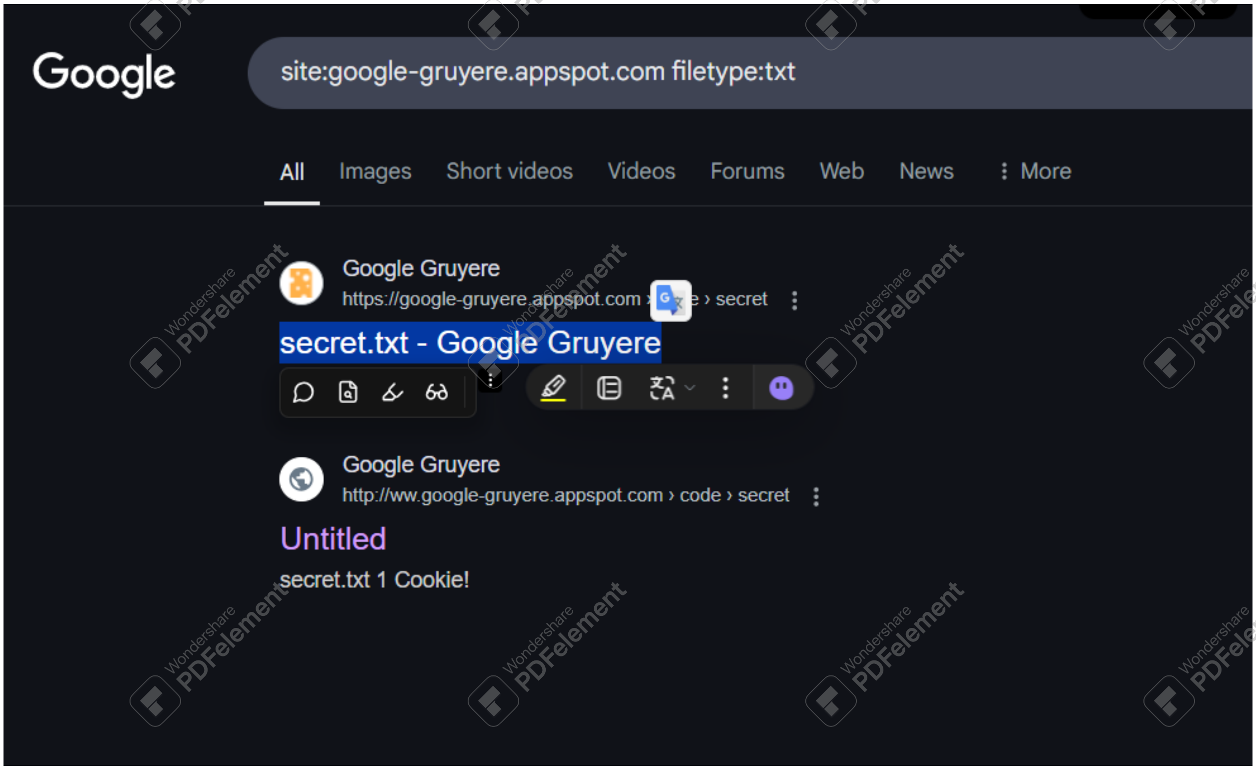
Google Dorks

Using the command: site:google-gruyere.appspot.com filetype:txt

Results: i. Found a TXT file titled " Secret.txt – Google Gruyere" hosted on the site.

ii. Found an untitled txt file hosted on the site.

Screenshot:



site:google-gruyere.appspot.com filetype:txt

Google Gruyere
https://google-gruyere.appspot.com › ... e › secret

secret.txt - Google Gruyere

Google Gruyere
http://ww.google-gruyere.appspot.com › code › secret

Untitled

secret.txt 1 Cookie!

2. using the command: site:google-gruyere.appspot.com filetype:pdf

Results:

1. Nothing found.

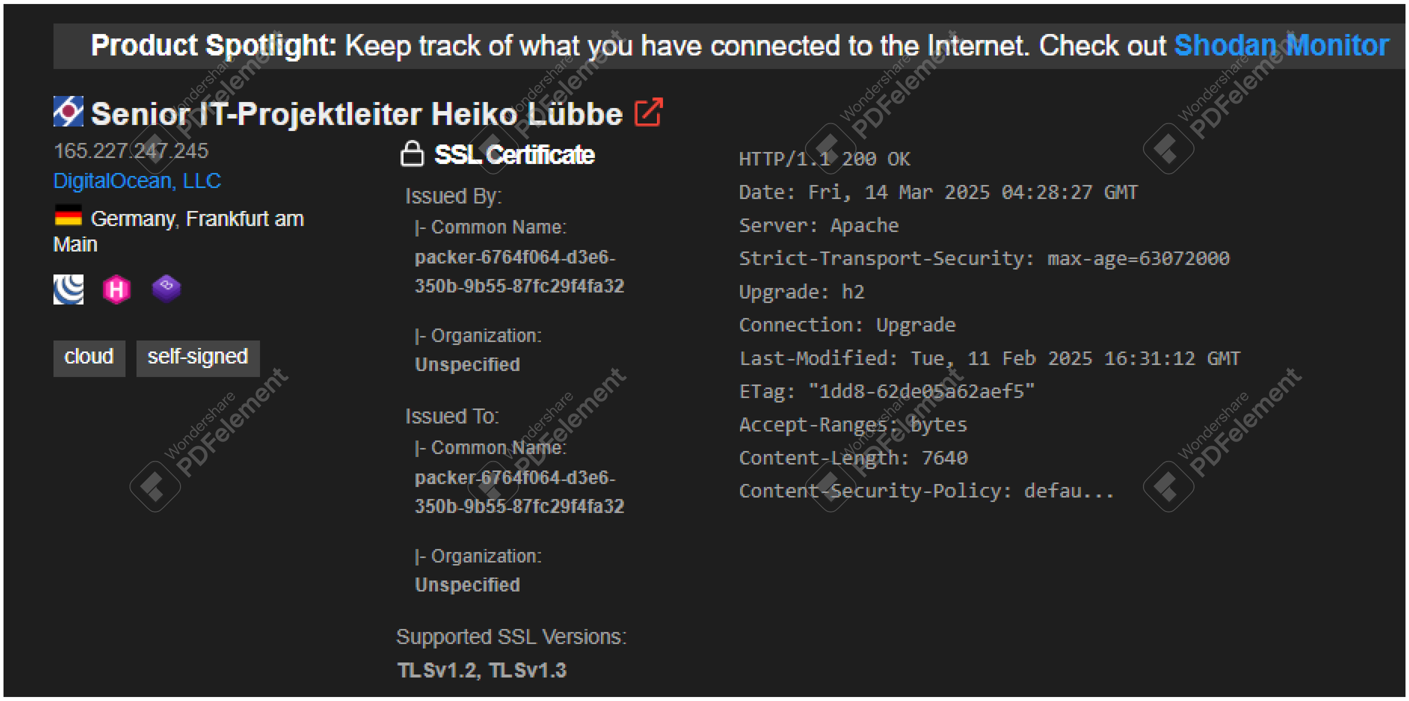
Shodan:

using site: google-gruyere.appspot.com

Results:

- Countries : Germany
- Ports : 433 (https)
- Server : Apache
- Connention : Upgrade
- Organization : DigitalOcean, LLC
- Products : apache httpd
- Website Titles : Senior IT-Projektleiter Heiko Lübbe
- Web technologies : Bootstrap , hugo , jQuery
- SSL / TLS version : tlsv1.2 and tlsv1.3

Screenshot:



Product Spotlight: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

Senior IT-Projektleiter Heiko Lübbe

165.227.247.245
DigitalOcean, LLC
Germany, Frankfurt am Main

cloud self-signed

SSL Certificate

Issued By:
|- Common Name:
packer-6764f064-d3e6-350b-9b55-87fc29f4fa32

|- Organization:
Unspecified

Issued To:
|- Common Name:
packer-6764f064-d3e6-350b-9b55-87fc29f4fa32

|- Organization:
Unspecified

Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Date: Fri, 14 Mar 2025 04:28:27 GMT
Server: Apache
Strict-Transport-Security: max-age=63072000
Upgrade: h2
Connection: Upgrade
Last-Modified: Tue, 11 Feb 2025 16:31:12 GMT
ETag: "1dd8-62de05a62aef5"
Accept-Ranges: bytes
Content-Length: 7640
Content-Security-Policy: defau...
```

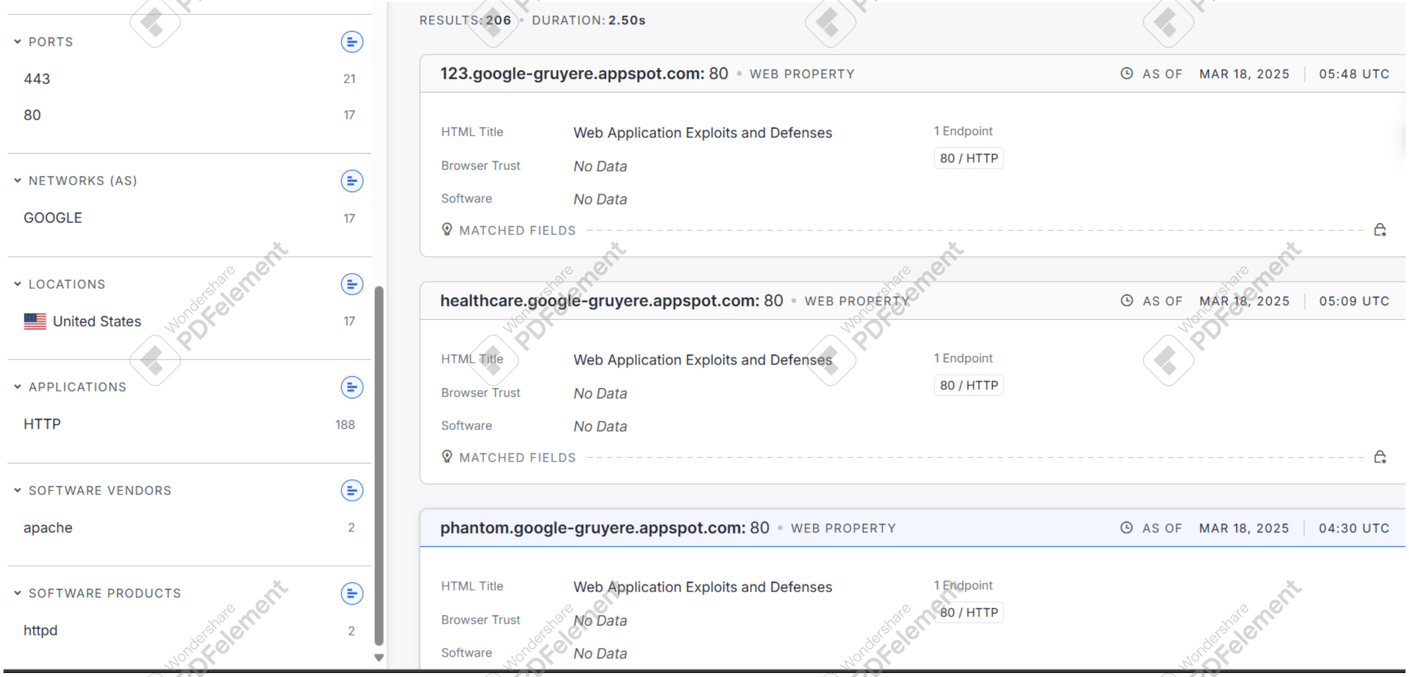
Censys

Using site : google-gruyere.appspot.com

Results:

- Ports : 443 (https) and 80 (http)
- Software vendors : apache
- Protocols : HTTP
- Transport protocols : TCP and QUIC
- Network : Google
- HTML title : Web Application Exploits and Defenses
- No Certificate Information Found.

Screenshot:



PORTS

443	21
80	17

NETWORKS (AS)

GOOGLE	17

LOCATIONS

United States	17

APPLICATIONS

HTTP	188

SOFTWARE VENDORS

apache	2

SOFTWARE PRODUCTS

httpd	2

RESULTS: 206 • DURATION: 2.50s

123.google-gruyere.appspot.com: 80 • WEB PROPERTY — AS OF MAR 18, 2025 | 05:48 UTC

HTML Title: Web Application Exploits and Defenses
Browser Trust: No Data
Software: No Data
1 Endpoint: 80 / HTTP
MATCHED FIELDS

healthcare.google-gruyere.appspot.com: 80 • WEB PROPERTY — AS OF MAR 18, 2025 | 05:09 UTC

HTML Title: Web Application Exploits and Defenses
Browser Trust: No Data
Software: No Data
1 Endpoint: 80 / HTTP
MATCHED FIELDS

phantom.google-gruyere.appspot.com: 80 • WEB PROPERTY — AS OF MAR 18, 2025 | 04:30 UTC

HTML Title: Web Application Exploits and Defenses
Browser Trust: No Data
Software: No Data
1 Endpoint: 80 / HTTP

Topic: Gather DNS, OS, and tracerouting information of Ips

Find the domain and subdomain using Netcraft:

1. Domain:

- Primary Domain: netcraft.com
- Subdomain: sitereport.netcraft.com

2. Netblock Owner:

- Cloudflare, Inc.

3. Hosting Country:

- United States (us)

4. IPv4 Address:

- 104.22.1.118

5.IPv6 Address:

- 2606:4700:10:0:0:6816:76

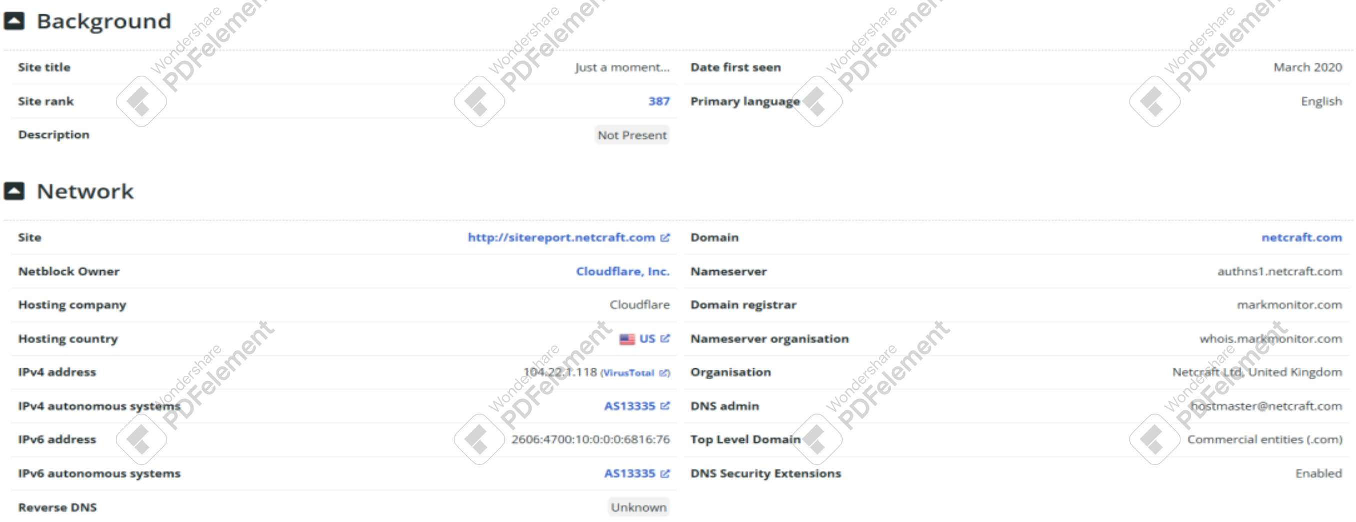
6. Domain Registrar:

- MarkMonitor

7. DNS Admin:

- hostmaster@netcraft.com

8. Top Level Domain: Commercial entities (.com)



Background

Site title	Just a moment...	Date first seen	March 2020
Site rank	387	Primary language	English
Description	Not Present		

Network

Site	http://sitereport.netcraft.com	Domain	netcraft.com
Netblock Owner	Cloudflare, Inc.	Nameserver	authns1.netcraft.com
Hosting company	Cloudflare	Domain registrar	markmonitor.com
Hosting country	US	Nameserver organisation	whois.markmonitor.com
IPv4 address	104.22.1.118 (VirusTotal)	Organisation	Netcraft Ltd, United Kingdom
IPv4 autonomous systems	AS13335	DNS admin	hostmaster@netcraft.com
IPv6 address	2606:4700:10:0:0:6816:76	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	AS13335	DNS Security Extensions	Enabled
Reverse DNS	Unknown		

Performing “whois” lookup of the website:

Domain Name: NETCRAFT.COM

Registry Domain ID: 509179_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.markmonitor.com

Registrar URL: http://www.markmonitor.com

Updated Date: 2025-01-06T17:21:04Z

Creation Date: 1994-10-18T04:00:00Z

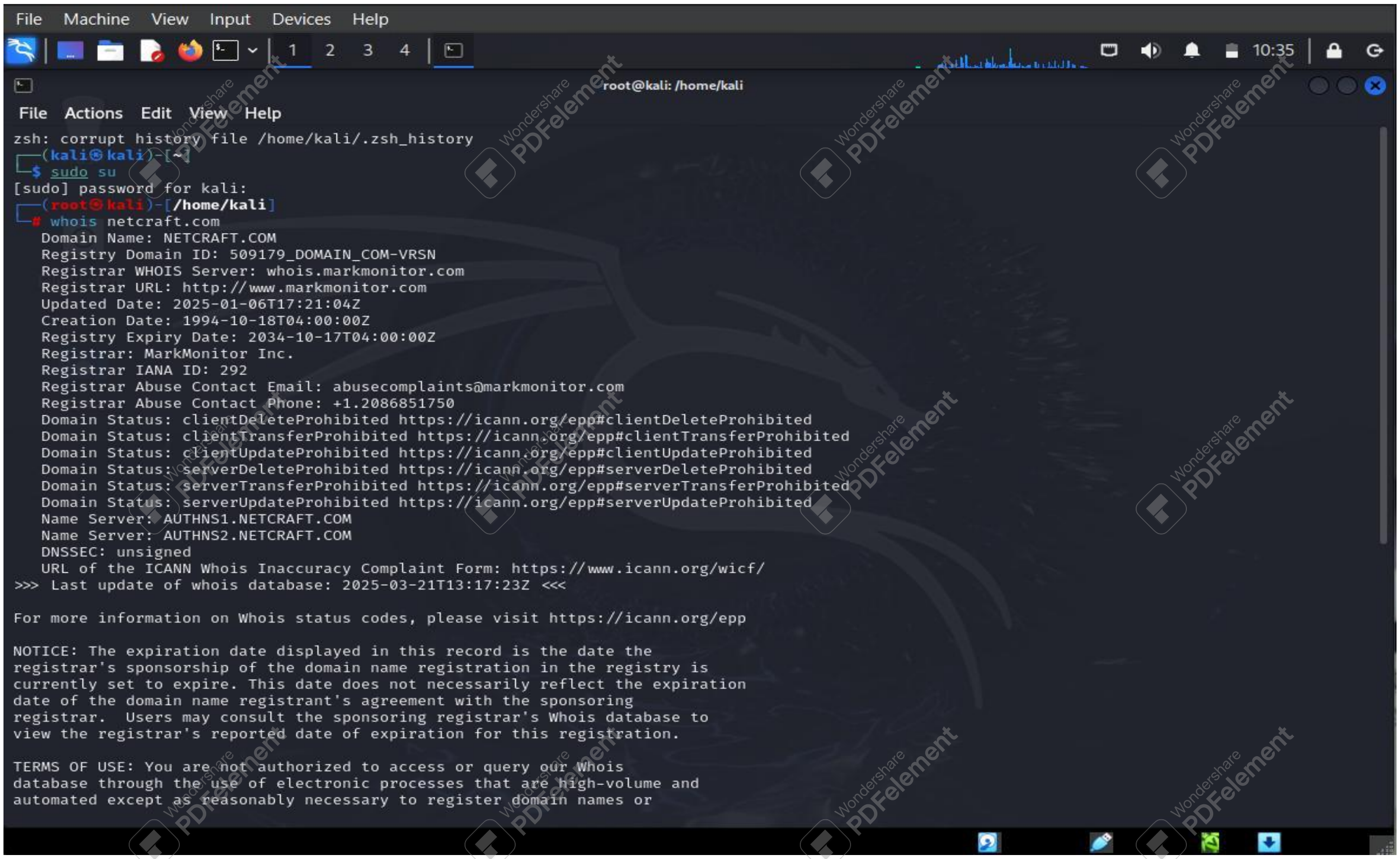
Registry Expiry Date: 2034-10-17T04:00:00Z

Registrar: MarkMonitor Inc.

Registrar IANA ID: 292

Registrar Abuse Contact Email: abusecomplaints@markmonitor.com Registrar Abuse Contact Phone: +1.2086851750

Screenshot:



File Machine View Input Devices Help
1 2 3 4
10:35
root@kali: /home/kali
File Actions Edit View Help

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# whois netcraft.com
   Domain Name: NETCRAFT.COM
   Registry Domain ID: 509179_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2025-01-06T17:21:04Z
   Creation Date: 1994-10-18T04:00:00Z
   Registry Expiry Date: 2034-10-17T04:00:00Z
   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: AUTHNS1.NETCRAFT.COM
   Name Server: AUTHNS2.NETCRAFT.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-03-21T13:17:23Z <<<

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
```

Use dig to gather DNS information

Review of the test :

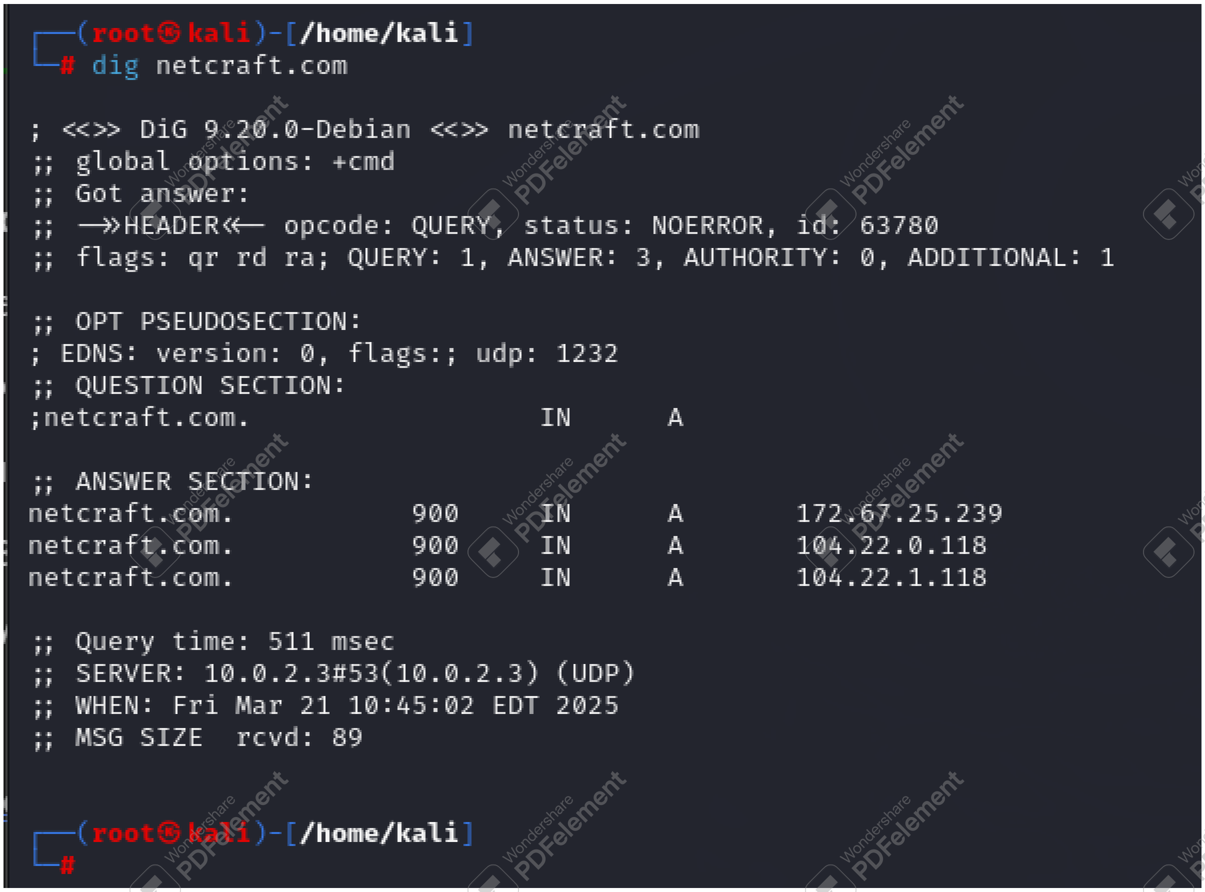
opcode: QUERY,

status: NOERROR,

id: 63780

SERVER: 10.0.2.3#53(10.0.2.3) (UDP)

Screenshot :



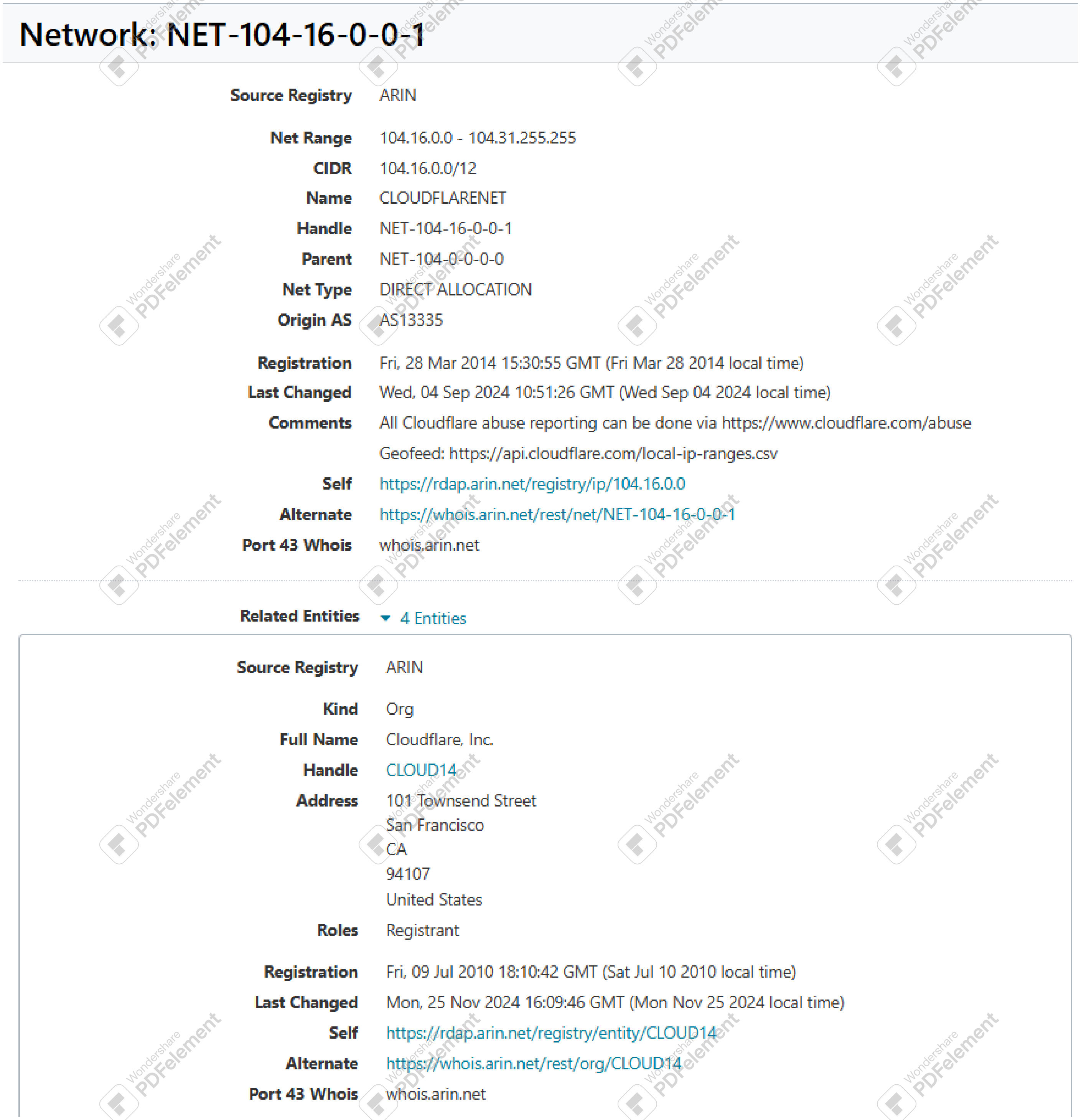
```
┌──(root㉿kali)-[/home/kali]
└─# dig netcraft.com

; <<>> DiG 9.20.0-Debian <<>> netcraft.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63780
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;netcraft.com.                  IN      A

;; ANSWER SECTION:
netcraft.com.           900     IN      A       172.67.25.239
netcraft.com.           900     IN      A       104.22.0.118
netcraft.com.           900     IN      A       104.22.1.118

;; Query time: 511 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Fri Mar 21 10:45:02 EDT 2025
;; MSG SIZE  rcvd: 89


┌──(root㉿kali)-[/home/kali]
└─#
```

Use the ARIN website to check the IP range:

IP Address: 104.22.1.118

Net Range: 104.16.0.0 - 104.31.255.255

Screenshot :



Network: NET-104-16-0-0-1

Source Registry	ARIN
Net Range	104.16.0.0 - 104.31.255.255
CIDR	104.16.0.0/12
Name	CLOUDFLARENET
Handle	NET-104-16-0-0-1
Parent	NET-104-0-0-0-0
Net Type	DIRECT ALLOCATION
Origin AS	AS13335
Registration	Fri, 28 Mar 2014 15:30:55 GMT (Fri Mar 28 2014 local time)
Last Changed	Wed, 04 Sep 2024 10:51:26 GMT (Wed Sep 04 2024 local time)
Comments	All Cloudflare abuse reporting can be done via https://www.cloudflare.com/abuse Geofeed: https://api.cloudflare.com/local-ip-ranges.csv
Self	https://rdap.arin.net/registry/ip/104.16.0.0
Alternate	https://whois.arin.net/rest/net/NET-104-16-0-0-1
Port 43 Whois	whois.arin.net

Related Entities ▾ 4 Entities

Source Registry	ARIN
Kind	Org
Full Name	Cloudflare, Inc.
Handle	CLOUD14
Address	101 Townsend Street San Francisco CA 94107 United States
Roles	Registrant
Registration	Fri, 09 Jul 2010 18:10:42 GMT (Sat Jul 10 2010 local time)
Last Changed	Mon, 25 Nov 2024 16:09:46 GMT (Mon Nov 25 2024 local time)
Self	https://rdap.arin.net/registry/entity/CLOUD14
Alternate	https://whois.arin.net/rest/org/CLOUD14
Port 43 Whois	whois.arin.net

Reconnaissance Report: Netcraft.com using Recon-ng

1. Objective

The goal of this activity is to gather publicly available information about the target domain **netcraft.com** using passive reconnaissance tools. Subdomains are enumerated using Recon-ng, and their IP addresses are resolved using Linux commands. This workflow simulates the **initial reconnaissance phase** of a penetration test while staying within legal OSINT limits.

2. Tools Used

- **Recon-ng v5.1.2** (OSINT framework)
- **Linux Terminal** (dig, host, ping)

Methodology:

1. Created workspace
2. Added domain target
3. Performed WHOIS lookup
4. Enumerated subdomains
5. Queried Certificate Transparency logs
6. Collected DNS information

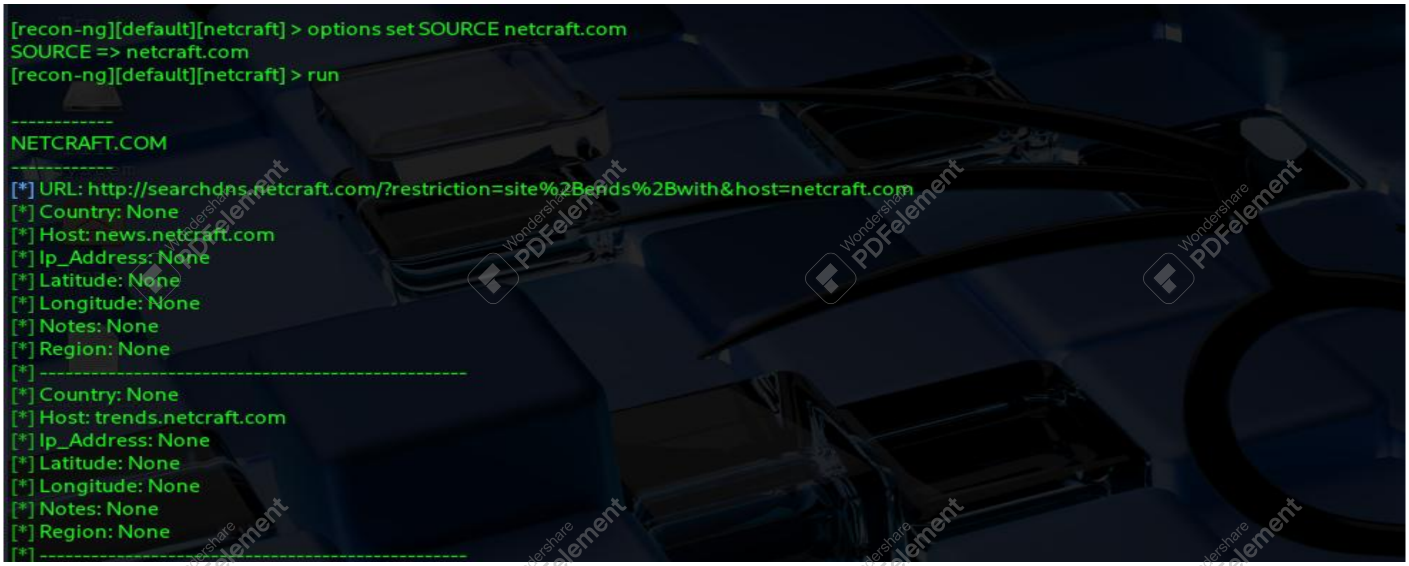
Commands Used:

```
1. recon-ng
2. workspaces create netcraft_recon
3. db insert domains --
4. modules load recon/domains-hosts/crtsh
5. set SOURCE netcraft.com
6. run
```

Findings:

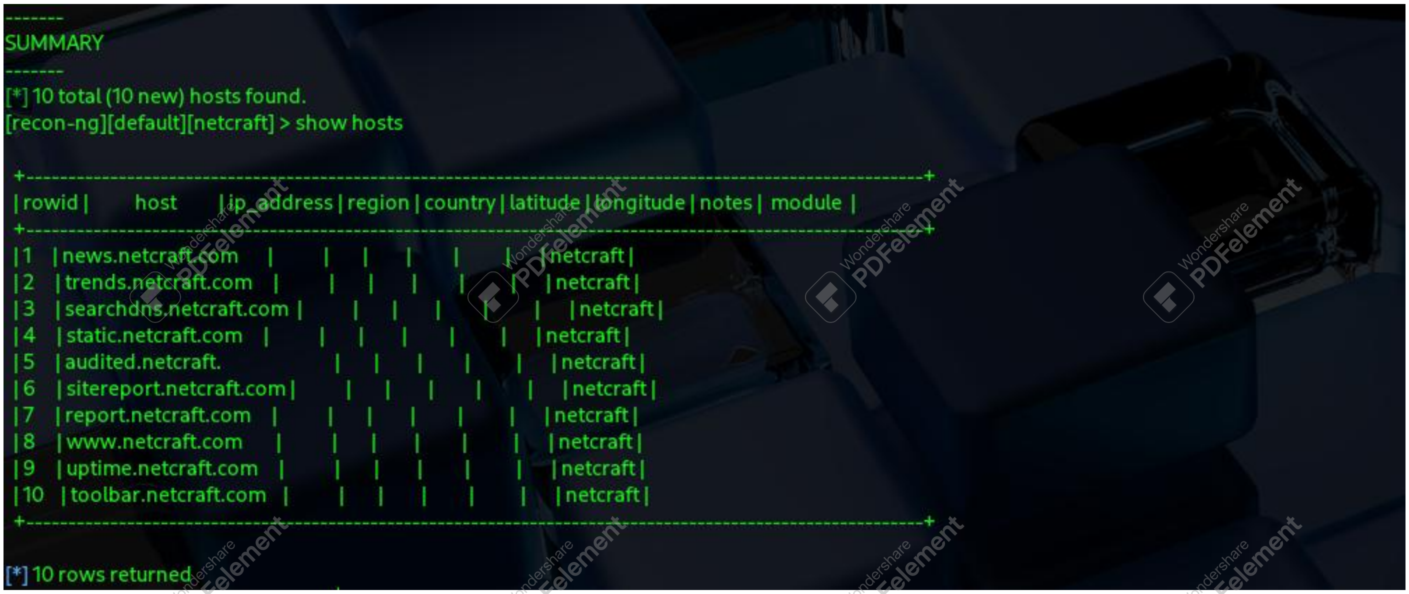
- Identified multiple subdomains
- Retrieved WHOIS data
- Gathered publicly available DNS information
- No intrusive scanning performed

Capture:
running successfully



```
[recon-ng][default][netcraft] > options set SOURCE netcraft.com
SOURCE => netcraft.com
[recon-ng][default][netcraft] > run

-----------
NETCRAFT.COM
-----------
[*] URL: http://searchdns.netcraft.com/?restriction=site%2Bends%2Bwith&host=netcraft.com
[*] Country: None
[*] Host: news.netcraft.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------
[*] Country: None
[*] Host: trends.netcraft.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------
```

Showing hosts –



```
-------
SUMMARY
-------
[*] 10 total (10 new) hosts found.
[recon-ng][default][netcraft] > show hosts

 +-------------------------------------------------------------------------------------------+
 | rowid |        host         | ip_address | region | country | latitude | longitude | notes |  module  |
 +-------------------------------------------------------------------------------------------+
 | 1     | news.netcraft.com      |            |        |         |          |           | netcraft |
 | 2     | trends.netcraft.com    |            |        |         |          |           | netcraft |
 | 3     | searchdns.netcraft.com |            |        |         |          |           | netcraft |
 | 4     | static.netcraft.com    |            |        |         |          |           | netcraft |
 | 5     | audited.netcraft.      |            |        |         |          |           | netcraft |
 | 6     | sitereport.netcraft.com|            |        |         |          |           | netcraft |
 | 7     | report.netcraft.com    |            |        |         |          |           | netcraft |
 | 8     | www.netcraft.com       |            |        |         |          |           | netcraft |
 | 9     | uptime.netcraft.com    |            |        |         |          |           | netcraft |
 | 10    | toolbar.netcraft.com   |            |        |         |          |           | netcraft |
 +-------------------------------------------------------------------------------------------+

[*] 10 rows returned
```

Resolve Subdomains to Ips :

Subdomain	IPv4 Address	IPv6 Address	Notes
news.netcraft.com	104.20.35.98, 172.66.147.145	–	Alias to `www.netcraft.com.cdn.cloudflare.net`
www.netcraft.com	104.20.35.98, 172.66.147.145	2606:4700:10::6814:2362, 2606:4700:10::ac42:9391	Main website
trends.netcraft.com	–	–	Discovered in Recon-ng