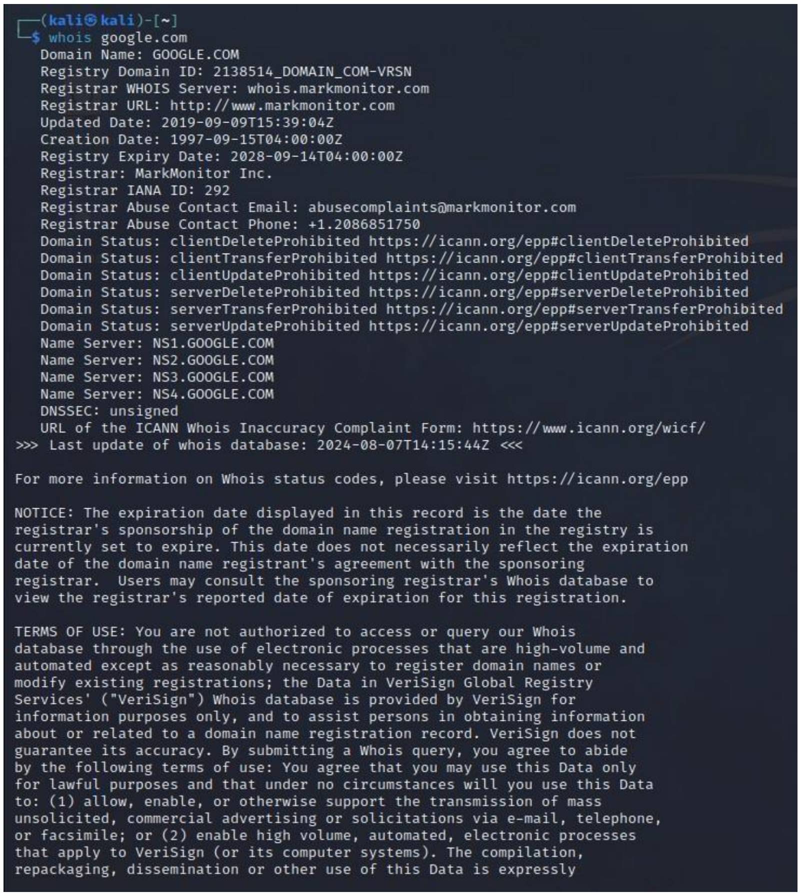
(PART - B)

(TO BE COMPLETED BY STUDENTS)

Roll.No. : A053	Name: Nishant Baruah
Sem: VII	Batch: 2
Date of Experiment : 06/08/24	Date of Submission: 06/08/24
Grade --	

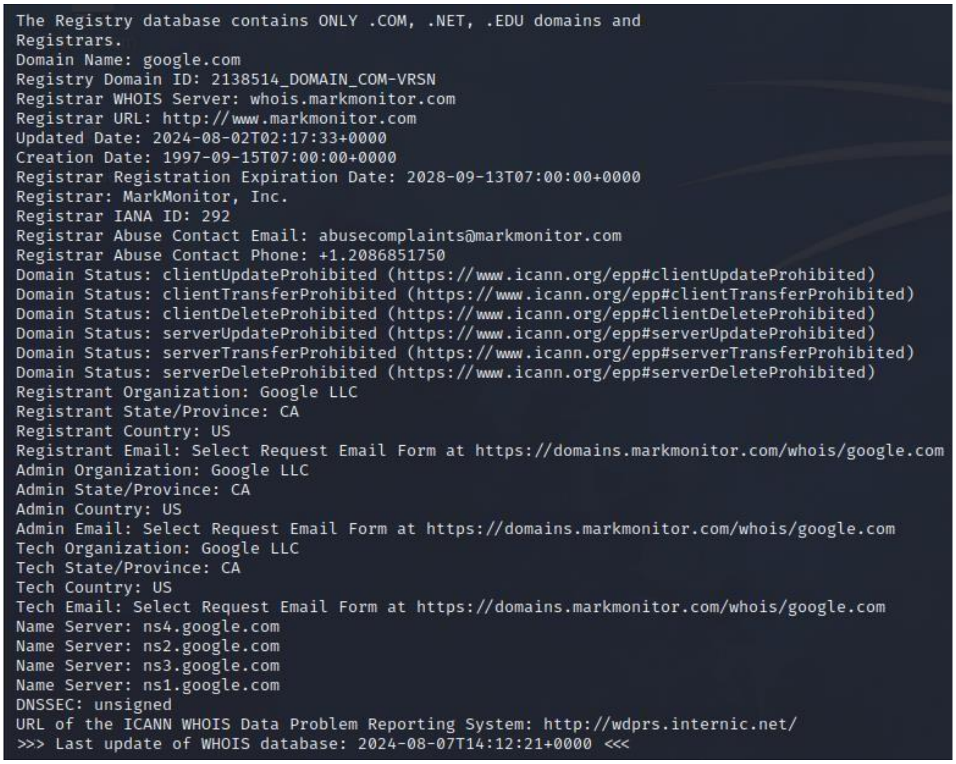
B. 1: Procedure of performed experiment

- **Whois –**



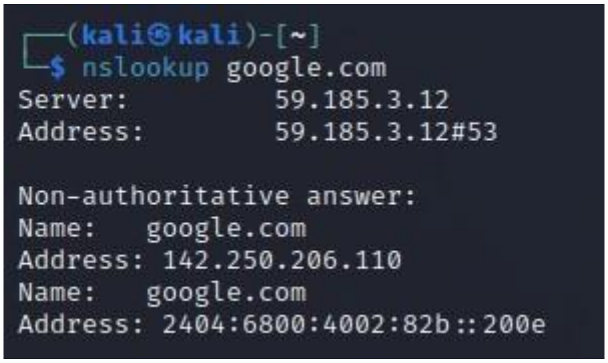
```
┌──(kali㉿kali)-[~]
└─$ whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   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: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-08-07T14:15:44Z <<<

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
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
```

-



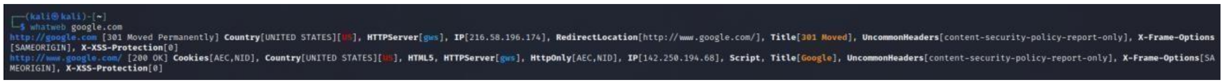
```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2024-08-02T02:17:33+0000
Creation Date: 1997-09-15T07:00:00+0000
Registrar Registration Expiration Date: 2028-09-13T07:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Google LLC
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Organization: Google LLC
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Name Server: ns4.google.com
Name Server: ns2.google.com
Name Server: ns3.google.com
Name Server: ns1.google.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-08-07T14:12:21+0000 <<<
```

- **Nslookup –**



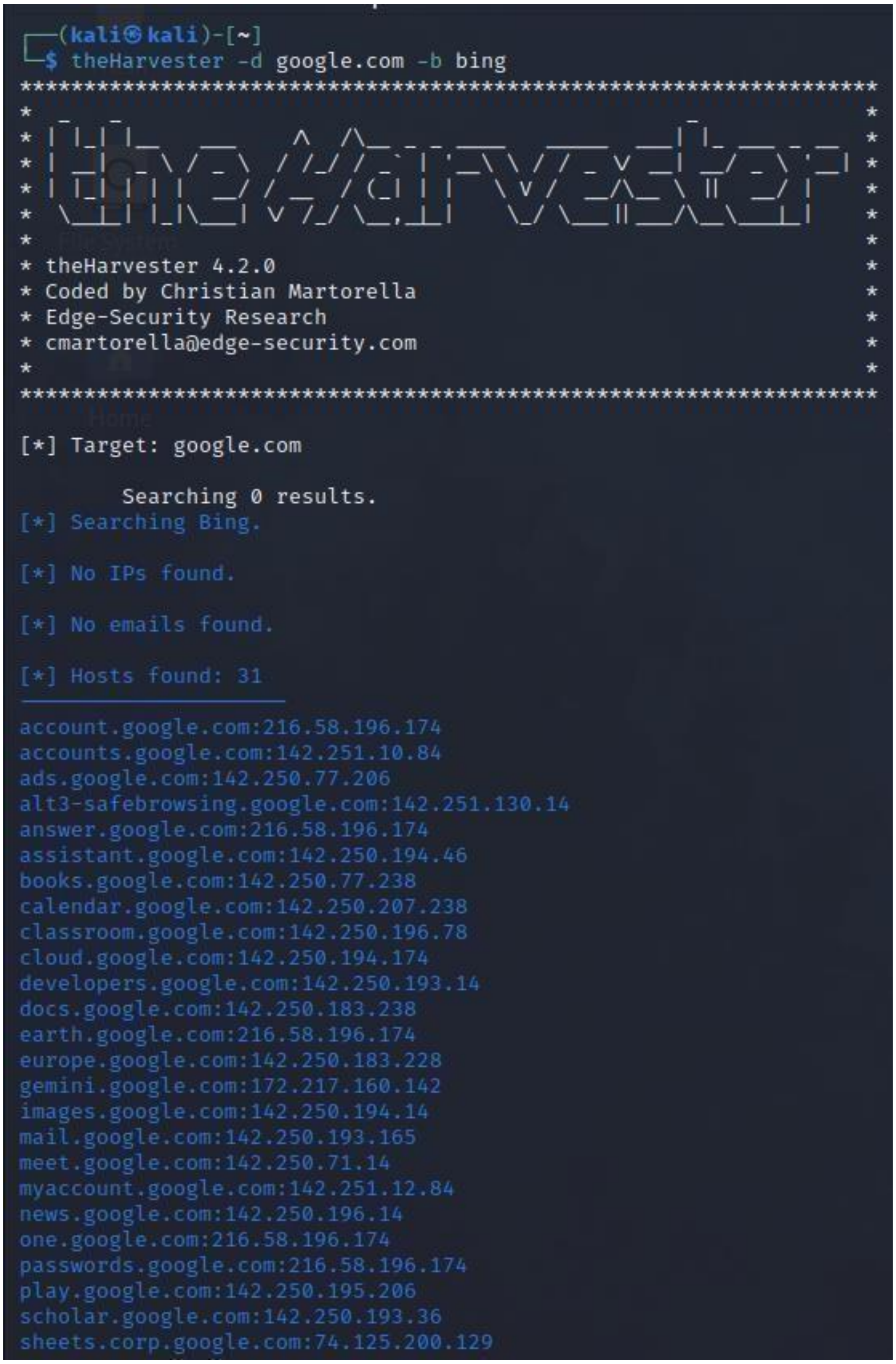
```
┌──(kali㉿kali)-[~]
└─$ nslookup google.com
Server:         59.185.3.12
Address:        59.185.3.12#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.206.110
Name:   google.com
Address: 2404:6800:4002:82b::200e
```

- **Whatweb –**



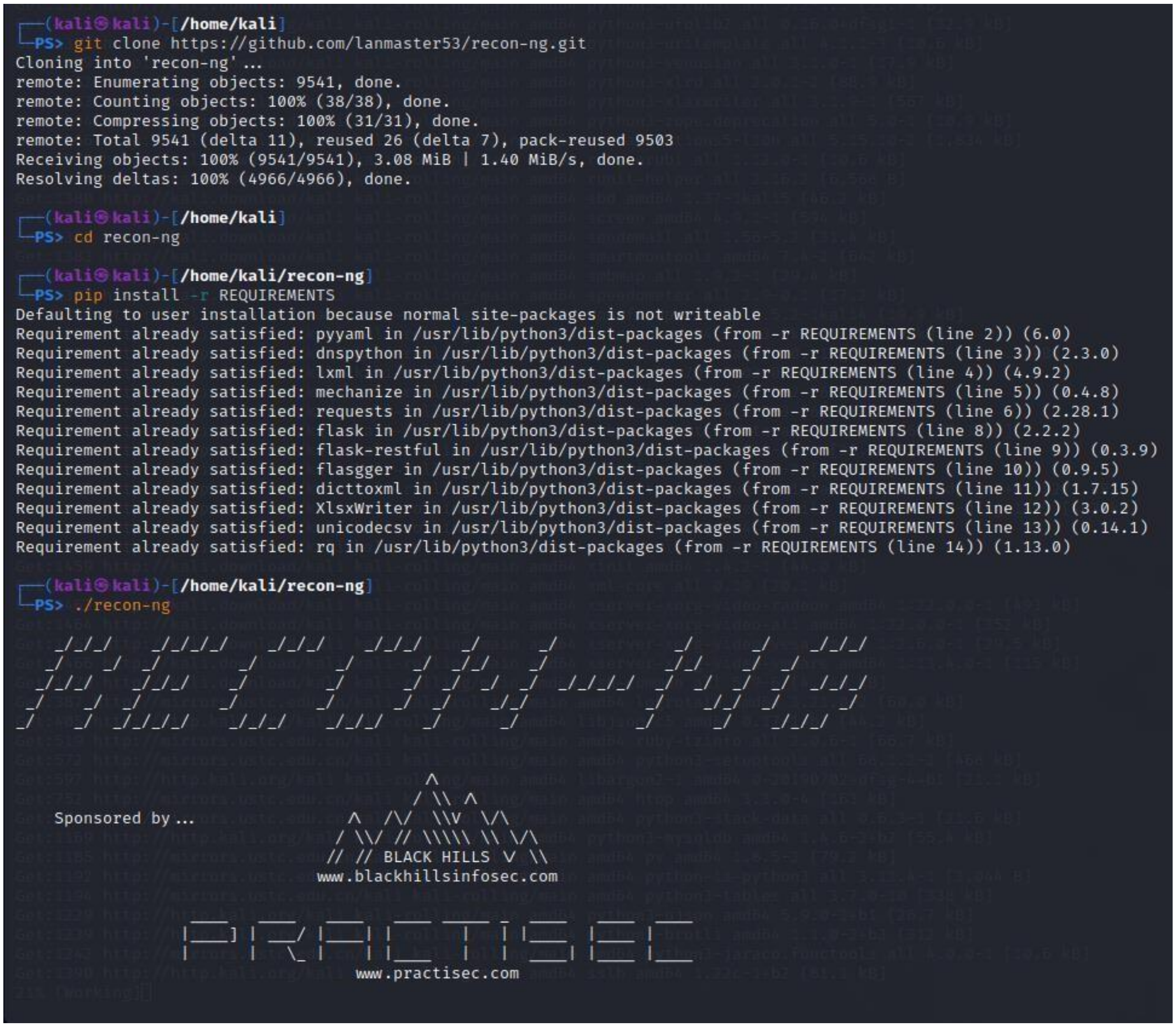
```
┌──(kali㉿kali)-[~]
└─$ whatweb google.com
http://google.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[gws], IP[216.58.196.174], RedirectLocation[http://www.google.com/], Title[301 Moved], UncommonHeaders[content-security-policy-report-only], X-Frame-Options
[SAMEORIGIN], X-XSS-Protection[0]
http://www.google.com/ [200 OK] Cookies[AEC,NID], Country[UNITED STATES][US], HTML5, HTTPServer[gws], HttpOnly[AEC,NID], IP[142.250.194.68], Script, Title[Google], UncommonHeaders[content-security-policy-report-only], X-Frame-Options[SA
MEORIGIN], X-XSS-Protection[0]
```

- **theHarvester –**

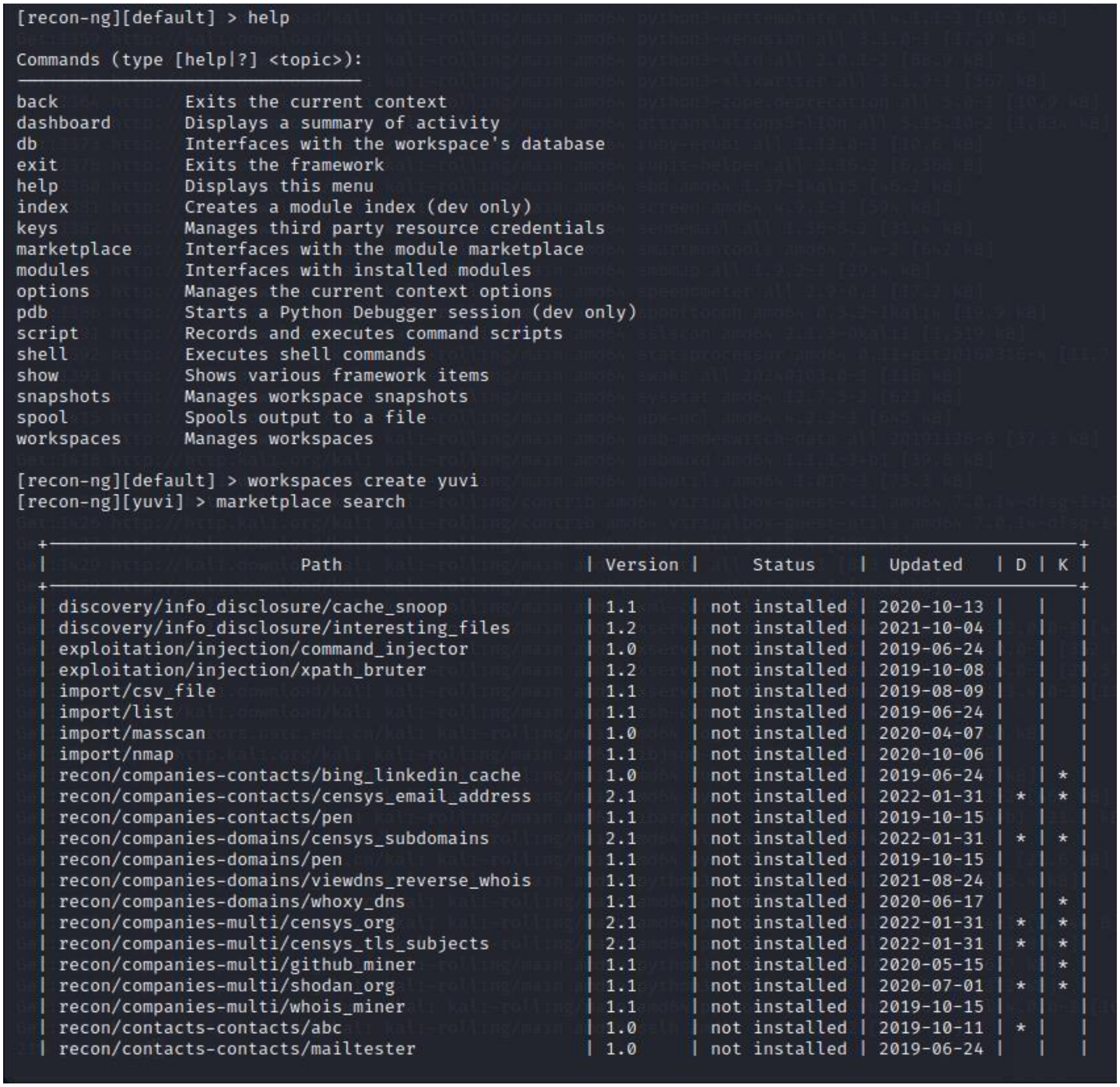


```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d google.com -b bing
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.2.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: google.com

        Searching 0 results.
[*] Searching Bing.

[*] No IPs found.

[*] No emails found.

[*] Hosts found: 31
---------------------
account.google.com:216.58.196.174
accounts.google.com:142.251.10.84
ads.google.com:142.250.77.206
alt3-safebrowsing.google.com:142.251.130.14
answer.google.com:216.58.196.174
assistant.google.com:142.250.194.46
books.google.com:142.250.77.238
calendar.google.com:142.250.207.238
classroom.google.com:142.250.196.78
cloud.google.com:142.250.194.174
developers.google.com:142.250.193.14
docs.google.com:142.250.183.238
earth.google.com:216.58.196.174
europe.google.com:142.250.183.228
gemini.google.com:172.217.160.142
images.google.com:142.250.194.14
mail.google.com:142.250.193.165
meet.google.com:142.250.71.14
myaccount.google.com:142.251.12.84
news.google.com:142.250.196.14
one.google.com:216.58.196.174
passwords.google.com:216.58.196.174
play.google.com:142.250.195.206
scholar.google.com:142.250.193.36
sheets.corp.google.com:74.125.200.129
```

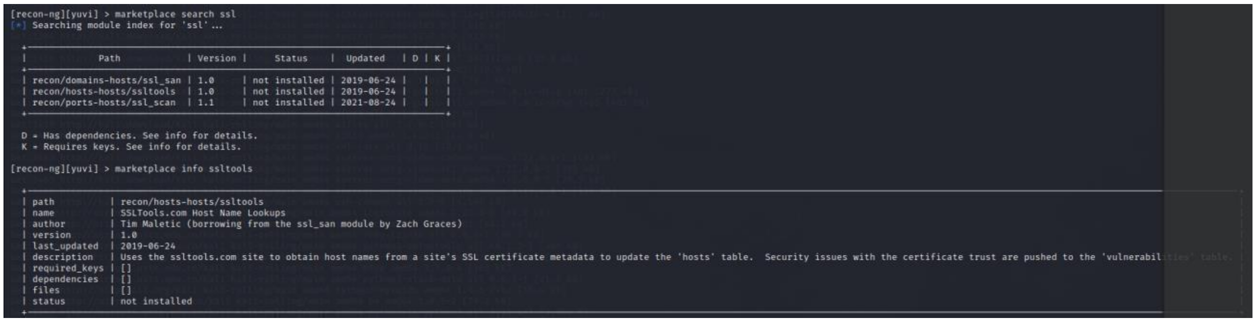
- **Recon-ng**



```
┌──(kali㉿kali)-[/home/kali]
└─PS> git clone https://github.com/lanmaster53/recon-ng.git
Cloning into 'recon-ng'...
remote: Enumerating objects: 9541, done.
remote: Counting objects: 100% (38/38), done.
remote: Compressing objects: 100% (31/31), done.
remote: Total 9541 (delta 11), reused 26 (delta 7), pack-reused 9503
Receiving objects: 100% (9541/9541), 3.08 MiB | 1.40 MiB/s, done.
Resolving deltas: 100% (4966/4966), done.

┌──(kali㉿kali)-[/home/kali]
└─PS> cd recon-ng

┌──(kali㉿kali)-[/home/kali/recon-ng]
└─PS> pip install -r REQUIREMENTS
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: pyyaml in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 2)) (6.0)
Requirement already satisfied: dnspython in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 3)) (2.3.0)
Requirement already satisfied: lxml in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 4)) (4.9.2)
Requirement already satisfied: mechanize in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 5)) (0.4.8)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 6)) (2.28.1)
Requirement already satisfied: flask in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 8)) (2.2.2)
Requirement already satisfied: flask-restful in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 9)) (0.3.9)
Requirement already satisfied: flasgger in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 10)) (0.9.5)
Requirement already satisfied: dicttoxml in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 11)) (1.7.15)
Requirement already satisfied: XlsxWriter in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 12)) (3.0.2)
Requirement already satisfied: unicodecsv in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 13)) (0.14.1)
Requirement already satisfied: rq in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 14)) (1.13.0)

┌──(kali㉿kali)-[/home/kali/recon-ng]
└─PS> ./recon-ng

    _/_/_/    _/_/_/_/    _/_/_/    _/_/_/    _/      _/            _/      _/    _/_/_/
   _/    _/  _/        _/        _/      _/  _/_/    _/            _/_/    _/  _/
  _/_/_/    _/_/_/    _/        _/      _/  _/  _/  _/  _/_/_/_/  _/  _/  _/  _/  _/_/_/
 _/    _/  _/        _/        _/      _/  _/    _/_/            _/    _/_/  _/      _/
_/    _/  _/_/_/_/    _/_/_/    _/_/_/    _/      _/            _/      _/    _/_/_/


                                          ^
                                         / \\ ^
    Sponsored by ...               ^  /\/  \\V  \/\
                                  / \\/ // \\\\\ \\ \/\
                                 // // BLACK HILLS V \\
                                www.blackhillsinfosec.com

                  ____   ____   ____   ____ _____ _  ____   ____  ____
                 |____] |___/  |____| |       |   | |____  |____ |
                 |      |   \_ |    | |____   |   |  ____| |____ |____
                                   www.practisec.com
```



```
[recon-ng][default] > help

Commands (type [help|?] <topic>):
---------------------------------
back            Exits the current context
dashboard       Displays a summary of activity
db              Interfaces with the workspace's database
exit            Exits the framework
help            Displays this menu
index           Creates a module index (dev only)
keys            Manages third party resource credentials
marketplace     Interfaces with the module marketplace
modules         Interfaces with installed modules
options         Manages the current context options
pdb             Starts a Python Debugger session (dev only)
script          Records and executes command scripts
shell           Executes shell commands
show            Shows various framework items
snapshots       Manages workspace snapshots
spool           Spools output to a file
workspaces      Manages workspaces

[recon-ng][default] > workspaces create yuvi
[recon-ng][yuvi] > marketplace search

  +---------------------------------------------------------------------------------------------------+
  |                        Path                          | Version |     Status    |  Updated   | D | K |
  +---------------------------------------------------------------------------------------------------+
  | discovery/info_disclosure/cache_snoop                | 1.1     | not installed | 2020-10-13 |   |   |
  | discovery/info_disclosure/interesting_files          | 1.2     | not installed | 2021-10-04 |   |   |
  | exploitation/injection/command_injector              | 1.0     | not installed | 2019-06-24 |   |   |
  | exploitation/injection/xpath_bruter                  | 1.2     | not installed | 2019-10-08 |   |   |
  | import/csv_file                                      | 1.1     | not installed | 2019-08-09 |   |   |
  | import/list                                          | 1.1     | not installed | 2019-06-24 |   |   |
  | import/masscan                                       | 1.0     | not installed | 2020-04-07 |   |   |
  | import/nmap                                          | 1.1     | not installed | 2020-10-06 |   |   |
  | recon/companies-contacts/bing_linkedin_cache         | 1.0     | not installed | 2019-06-24 |   | * |
  | recon/companies-contacts/censys_email_address        | 2.1     | not installed | 2022-01-31 | * | * |
  | recon/companies-contacts/pen                         | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/companies-domains/censys_subdomains            | 2.1     | not installed | 2022-01-31 | * | * |
  | recon/companies-domains/pen                          | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/companies-domains/viewdns_reverse_whois        | 1.1     | not installed | 2021-08-24 |   |   |
  | recon/companies-domains/whoxy_dns                    | 1.1     | not installed | 2020-06-17 |   | * |
  | recon/companies-multi/censys_org                     | 2.1     | not installed | 2022-01-31 | * | * |
  | recon/companies-multi/censys_tls_subjects            | 2.1     | not installed | 2022-01-31 | * | * |
  | recon/companies-multi/github_miner                   | 1.1     | not installed | 2020-05-15 |   | * |
  | recon/companies-multi/shodan_org                     | 1.1     | not installed | 2020-07-01 | * | * |
  | recon/companies-multi/whois_miner                    | 1.1     | not installed | 2019-10-15 |   |   |
  | recon/contacts-contacts/abc                          | 1.0     | not installed | 2019-10-11 | * |   |
  | recon/contacts-contacts/mailtester                   | 1.0     | not installed | 2019-06-24 |   |   |
```



```
[recon-ng][yuvi] > marketplace search ssl
[*] Searching module index for 'ssl'...

  +-----------------------------------------------------------------------------------+
  |            Path              | Version |     Status    |  Updated   | D | K |
  +-----------------------------------------------------------------------------------+
  | recon/domains-hosts/ssl_san  | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/hosts-hosts/ssltools   | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/ports-hosts/ssl_scan   | 1.1     | not installed | 2021-08-24 |   |   |
  +-----------------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][yuvi] > marketplace info ssltools

  +---------------------------------------------------------------------------------------------------
  | path          | recon/hosts-hosts/ssltools
  | name          | SSLTools.com Host Name Lookups
  | author        | Tim Maletic (borrowing from the ssl_san module by Zach Graces)
  | version       | 1.0
  | last_updated  | 2019-06-24
  | description   | Uses the ssltools.com site to obtain host names from a site's SSL certificate metadata to update the 'hosts' table.  Security issues with the certificate trust are pushed to the 'vulnerabilities' table.
  | required_keys | []
  | dependencies  | []
  | files         | []
  | status        | not installed
  +---------------------------------------------------------------------------------------------------
```

B.2: Observations and Learning’s:

In the realm of cybersecurity and information gathering, several tools prove indispensable for a comprehensive analysis. `whois` is a fundamental tool for retrieving domain registration information, revealing the ownership details and the administrative contacts of a domain, which aids in tracing the origin and legitimacy of a website. `nslookup` facilitates querying DNS records, providing insights into the IP addresses associated with domain names, which is crucial for network troubleshooting and understanding domain infrastructures. `theHarvester` excels in gathering open-source intelligence (OSINT) by scraping various public data sources to uncover email addresses, subdomains, and other valuable information associated with a target domain. `p0f` stands out in passive fingerprinting, identifying operating systems and network characteristics of hosts without actively probing them, thereby minimizing detection risks. `recon-ng` is a powerful, modular reconnaissance framework that integrates with numerous sources and APIs, allowing for extensive data collection and analysis within a single, versatile interface. Lastly, `sublist3r` specializes in enumerating subdomains, helping security professionals map out the full landscape of a target domain's online presence, which is essential for identifying potential attack vectors. Together, these tools form a robust toolkit for any cybersecurity professional, providing critical insights and aiding in the protection and analysis of digital assets.

B.3: Conclusion:

In conclusion, mastering tools such as whois, nslookup, theHarvester, p0f, recon-ng, and `sublist3r is pivotal for anyone involved in cybersecurity and information gathering. Each tool offers unique capabilities that complement one another, from identifying domain ownership and querying DNS records to collecting open-source intelligence and performing passive network reconnaissance. The integration of these tools into a security professional's workflow not only enhances the thoroughness and efficiency of their investigations but also strengthens their ability to identify and mitigate potential security threats. By leveraging the comprehensive insights provided by these tools, cybersecurity practitioners can build a more secure and resilient digital environment.