

Footprinting and Reconnaissance

Lab Manual

Hacking with

RANJITH ADLAKADI

THE DOCUMENT INCLUDES ADDITIONAL
PRACTICALS WHICH MAY OR MAY NOT BE COVERED
IN THE COURSE

INDEX

S. No.	Practical Name	Page No.
1	Finding domain registration details with Whois tool	1
2	Extracting Emails and subdomains details using the harvester	2
3	To find out targets IP address using IP tracking technique	3
4	Footprinting domain using Recon-ng tool	5
5	Google Dorks	7

Practical 1: Finding domain registration details with Whois tool

WHOIS is used to gather information related to the domain name and DNS details of the target.

Enter the following command to perform **Whois** operation on target. In this case, we are targeting **hackerschool.in**

```
root@kali:~# whois hackerschool.in
Domain Name: HACKERSCHOOL.IN
Registry Domain ID: D5148917-AFIN
Registrar WHOIS Server:
Registrar URL: http://indialinks.com
Updated Date: 2017-10-14T08:41:44Z
Creation Date: 2011-07-06T07:49:29Z
Registry Expiry Date: 2021-07-06T07:49:29Z
Registrar Registration Expiration Date:
Registrar: India Links Web Hosting Pvt Ltd
Registrar IANA ID: 1487
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Reseller:
Domain Status: clientTransferProhibited
Domain Status: clientUpdateProhibited
Registrant Organization: hackerschool
Registrant State/Province: A P
Registrant Country: IN
Name Server: NS1.JUSTHOST.COM
Name Server: NS2.JUSTHOST.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2018-07-12T14:12:19Z <<<
```

Practical 2: Extracting Emails and subdomains details using the harvester

This tool is to gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like Google, Bing and other search engines.

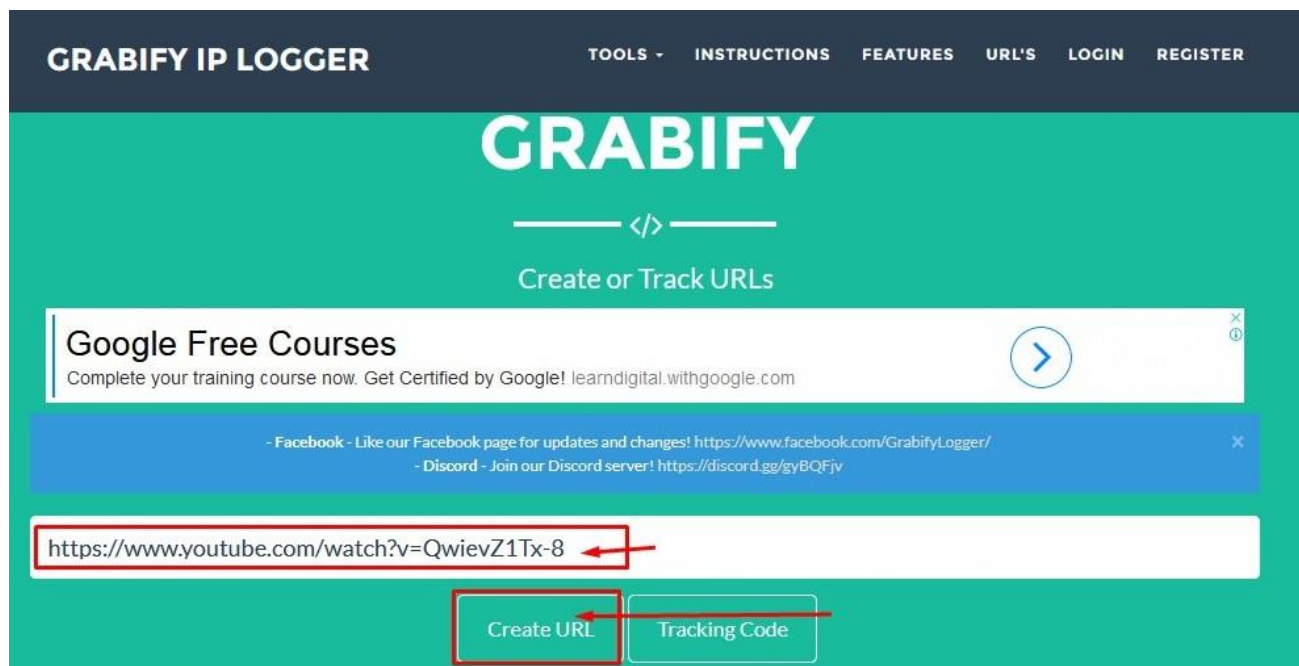
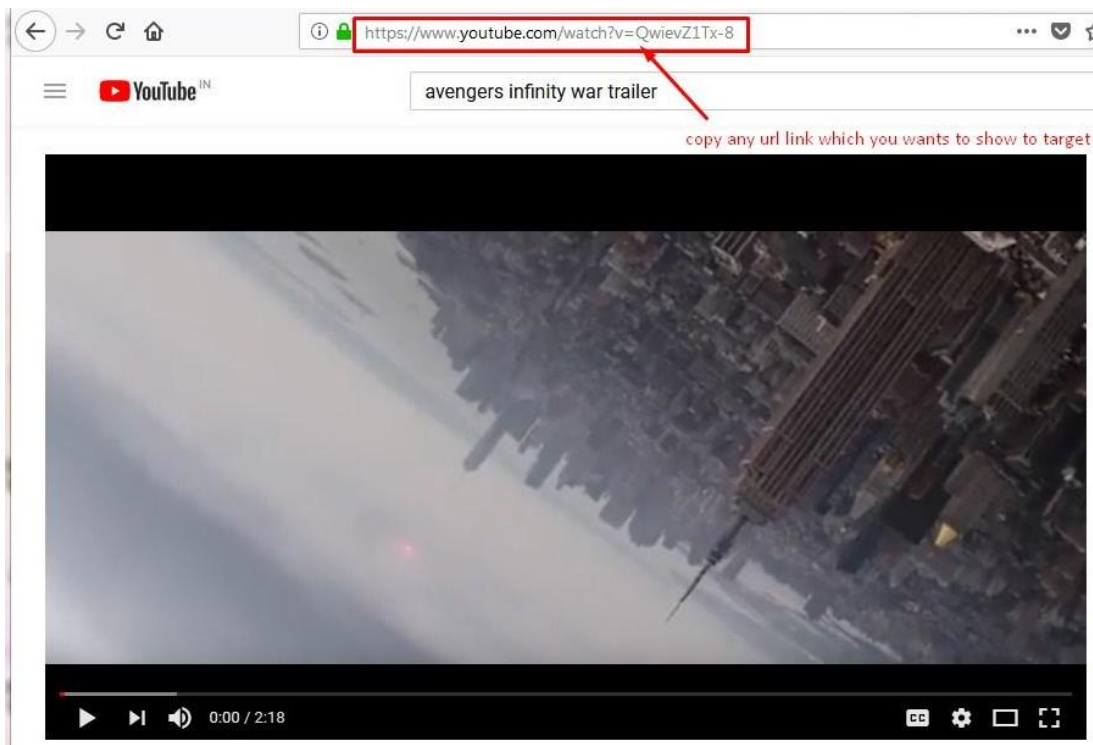
```
root@kali:~# theharvester -d example.com -l 1000 -b all
```

```
[+] Emails found:  
-----  
'localpart.ending.with.dot.@example.com  
09student@station09.example.com  
111@example.com  
123@example.com  
210231012014@example.com  
27462137@example.com  
44FC-4A7D-0B4E-A202-70C2-A5E6-E764-F7D6-key@example.com  
456@example.com  
555-555-0199@example.com  
769213cd5cf34c2ea4d658c300d4b094@example.com  
789@example.com  
Alice@example.com
```

Practical 3: To find out targets IP address using IP tracking technique.

Visit Grabify IP logging website <https://grabify.link/>

This website creates a tracking link which helps in identifying targets IP address. To perform this task, we are trying to convince our target to click on it tracking link that redirects target towards a youtube video. Create an IP tracking link by using grabify website; it requires valid URL (In this case we are converting youtube video link as an IP tracking link)



After clicking on **Create URL** button, the website generates IP tracking URL displayed in **New URL section**, which you can share with a target to grab IP address.

LINK INFORMATION:

Select Domain Name: [Click here](#)

(All custom links will stay active)

Original URL	https://www.youtube.com/watch?v=QwievZ1Tx-8
New URL New (Send them this link) Copy	https://grabify.link/PNQWBS Change domain/Make a custom link
Other Links (or this link)	View Other link Shorteners
Tracking Code	OOGMMW
Access Link	https://grabify.link/track/OOGMMW

If the target click on the link, the target's IP address will be displayed on the same page as shown below

RESULTS: 1

Note: If you have posted your link on Facebook, Twitter, or in a URL shortener, you may see results from various "bots" (BitlyBot, FacebookBot, etc.)

Pages: 1

Hide Bots

Date/Time	IP Address	Country 🌐	User Agent (Hover or tap for more information)	Referring URL	Host Name	ISP
2018-05-19 10:15:42	183.83.92.232	India, Hyderabad	Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0	<i>no referrer</i>	broadband.actcorp.in	Beam Telecom Pvt Ltd

Pages: 1

Page loaded in: 0.30750203132629

Practical 4: Footprinting domain using Recon-ng tool

To launch the recon-ng tool, execute the following command in terminal

```
root@kali:~# recon-ng
```

Execute the below command, to list out the modules.

```
Sponsored by...
                ^
              ^ ^
            ^ ^ ^
          ^ ^ ^ ^
        // // BLACK HILLS // //
        www.blackhillsinfosec.com

[recon-ng v4.9.2, Tim Tomes (@LaNMaSteR53)]

[77] Recon modules
[8] Reporting modules
[2] Import modules
[2] Exploitation modules
[2] Discovery modules

[recon-ng][default] > show modules
```

```
recon/contacts-profiles/fullcontact
recon/credentials-credentials/adobe
recon/credentials-credentials/bozocrack
recon/credentials-credentials/hashe_org
recon/domains-contacts/metacrawler
recon/domains-contacts/pgp_search
recon/domains-contacts/whois_pocs
recon/domains-credentials/pwnedlist/account_creds
recon/domains-credentials/pwnedlist/api_usage
recon/domains-credentials/pwnedlist/domain_creds
recon/domains-credentials/pwnedlist/domain_ispwned
recon/domains-credentials/pwnedlist/leak_lookup
recon/domains-credentials/pwnedlist/leak5_dump
recon/domains-domains/brute_suffix
recon/domains-hosts/bing_domain_api
recon/domains-hosts/bing_domain_web
recon/domains-hosts/brute_hosts
recon/domains-hosts/builtwith
recon/domains-hosts/certificate_transparency
recon/domains-hosts/google_site_api
recon/domains-hosts/google_site_web
```

To use a module, Execute the following command

```
[recon-ng][default] > use recon/domains-hosts/bing_domain_web
```

Execute the **show options** command, to view the list of options.

```
[recon-ng][default][bing_domain_web] > show options

Name      Current Value  Required  Description
-----
SOURCE    default       yes       source of input (see 'show info' for details)

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

Execute **set SOURCE <domain name>** command, to set the domain address as a source

Example: **set SOURCE juggyboy.com**

```
[recon-ng][default][bing_domain_web] > set source juggyboy.com
SOURCE => juggyboy.com
```

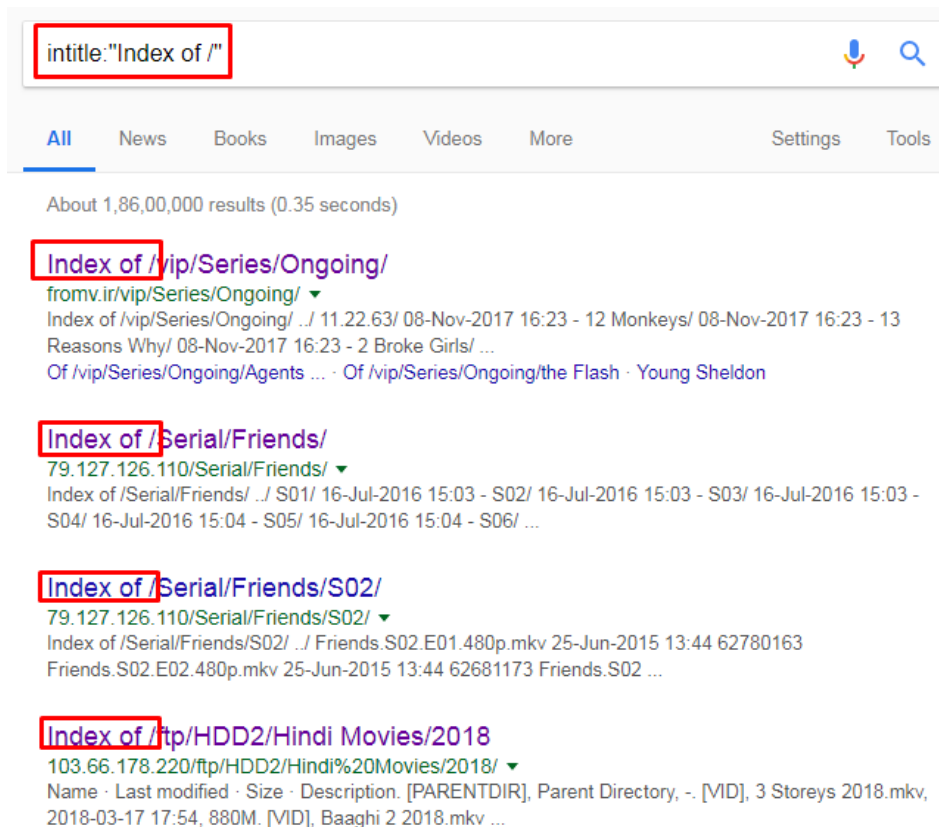
Execute the **run** command, to start the search for domains

```
[recon-ng][default][bing_domain_web] > run
-----
JUGGYBOY.COM
-----
[*] URL: https://www.bing.com/search?first=0&q=domain%3Ajuggyboy.com
[*] [host] www.juggyboy.com (<blank>)
[*] Sleeping to avoid lockout...
[*] URL: https://www.bing.com/search?first=0&q=domain%3Ajuggyboy.com+-domain%3Awww.juggyboy.com
[*] [host] notes.juggyboy.com (<blank>)
[*] Sleeping to avoid lockout...
[*] URL: https://www.bing.com/search?first=0&q=domain%3Ajuggyboy.com+-domain%3Awww.juggyboy.com
-----
SUMMARY
-----
[*] 2 total (0 new) hosts found.
[recon-ng][default][bing_domain_web] > □
```

Practical 5: Google Dorks

Google dorks are used to retrieving web pages that contain a specific term.

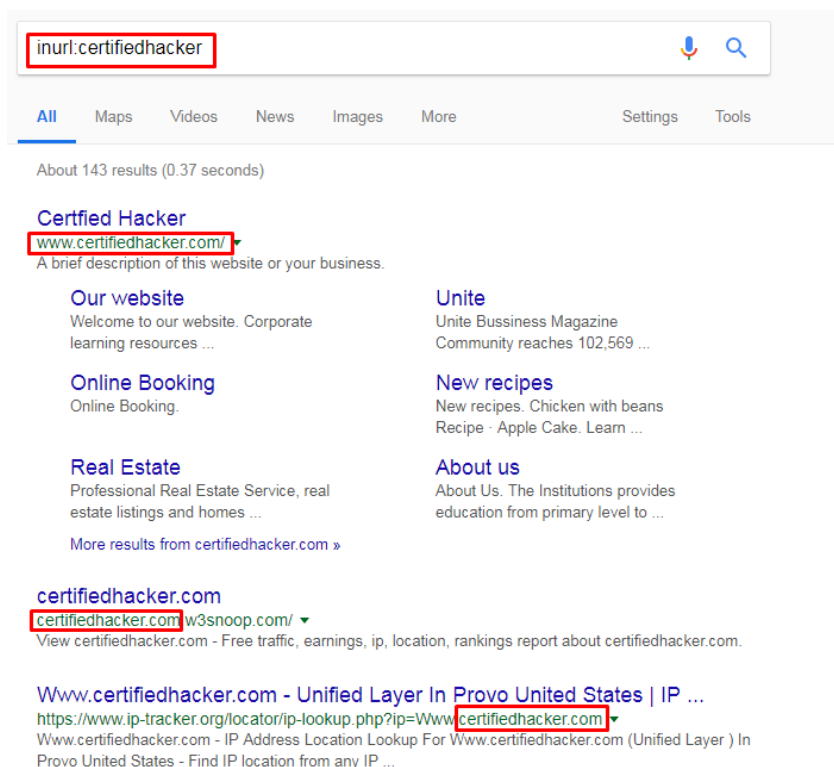
1. If you search for ***intitle:"Index of/"*** on google search bar, it will display those pages that contain the term "Index of/" in the title of the website.



The screenshot shows a Google search interface with the query `intitle:"Index of /"` entered in the search bar. The search results are displayed below, showing several entries with their titles and snippets. The titles are highlighted with red boxes:

- Index of /vip/Serial/Ongoing/**
fromv.ir/vip/Serial/Ongoing/ ...
Index of /vip/Serial/Ongoing/ .../ 11.22.63/ 08-Nov-2017 16:23 - 12 Monkeys/ 08-Nov-2017 16:23 - 13 Reasons Why/ 08-Nov-2017 16:23 - 2 Broke Girls/ ...
Of /vip/Serial/Ongoing/Agents ... - Of /vip/Serial/Ongoing/the Flash - Young Sheldon
- Index of /Serial/Friends/**
79.127.126.110/Serial/Friends/ ...
Index of /Serial/Friends/ .../ S01/ 16-Jul-2016 15:03 - S02/ 16-Jul-2016 15:03 - S03/ 16-Jul-2016 15:03 - S04/ 16-Jul-2016 15:04 - S05/ 16-Jul-2016 15:04 - S06/ ...
- Index of /Serial/Friends/S02/**
79.127.126.110/Serial/Friends/S02/ ...
Index of /Serial/Friends/S02/ .../ Friends.S02.E01.480p.mkv 25-Jun-2015 13:44 62780163
Friends.S02.E02.480p.mkv 25-Jun-2015 13:44 62681173 Friends.S02 ...
- Index of /ftp/HDD2/Hindi Movies/2018**
103.66.178.220/ftp/HDD2/Hindi%20Movies/2018/ ...
Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -, [VID], 3 Storeys 2018.mkv, 2018-03-17 17:54, 880M. [VID], Baaghi 2 2018.mkv ...

2. ***inurl:certifiedhacker*** will result in displaying those pages that contain the term "certifiedhacker" in the URL.



The screenshot shows a Google search interface with the query `inurl:certifiedhacker` entered in the search bar. The search results are displayed below, showing several entries with their titles and snippets. The titles are highlighted with red boxes:

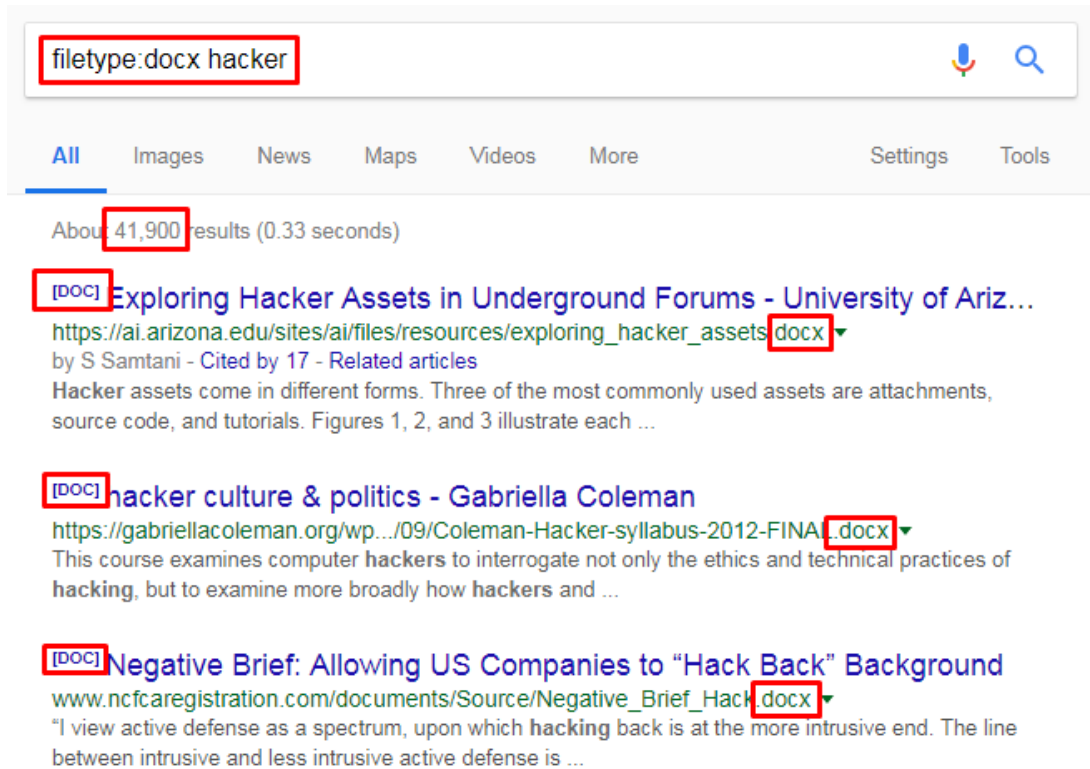
- Certified Hacker**
www.certifiedhacker.com/ ...
A brief description of this website or your business.
- Our website**
Welcome to our website. Corporate learning resources ...
- Online Booking**
Online Booking.
- Real Estate**
Professional Real Estate Service, real estate listings and homes ...
- Unite**
Unite Bussiness Magazine
Community reaches 102,569 ...
- New recipes**
New recipes. Chicken with beans
Recipe · Apple Cake. Learn ...
- About us**
About Us. The Institutions provides education from primary level to ...

More results from certifiedhacker.com »

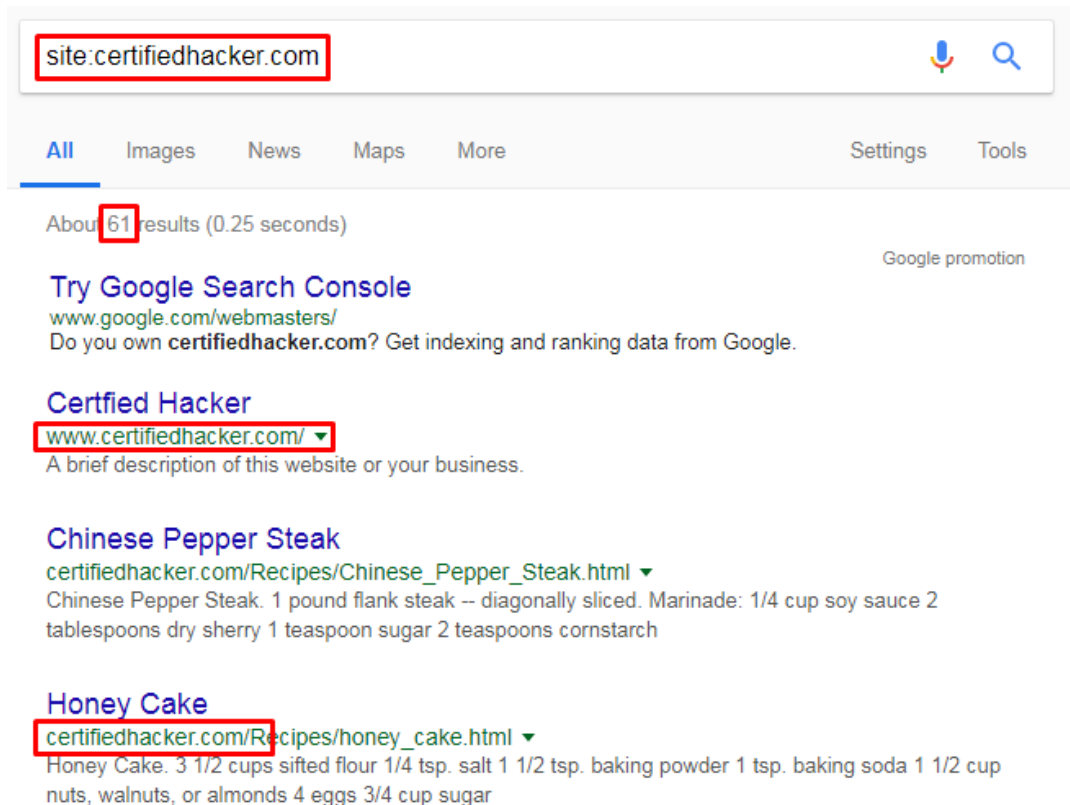
- certifiedhacker.com**
certifiedhacker.com/w3snoop.com/ ...
View certifiedhacker.com - Free traffic, earnings, ip, location, rankings report about certifiedhacker.com.
- Www.certifiedhacker.com - Unified Layer In Provo United States | IP ...**
<https://www.ip-tracker.org/locator/ip-lookup.php?ip=Www.certifiedhacker.com> ...
Www.certifiedhacker.com - IP Address Location Lookup For Www.certifiedhacker.com (Unified Layer) In Provo United States - Find IP location from any IP ...

3. To find out files of a specific format, we can use **filetype:** followed by file type (pdf, docx, xlsx) and keyword.

For example, **filetype:docx hacker** will display all word documents that contain word hacker.



4. **site:certifiedhacker.com** will display the results that contain the term "certifiedhacker" in the website URL.



5. ***allintitle: trojan definition*** will return results that contain words trojan and definition in web page titles.

Refer following web pages for advanced Google operators

http://www.googleguide.com/advanced_operators_reference.html

<http://www.exploit-db.com>