



Reconnaissance (Information Gathering)

Day1_info.md



Recall

LAST TIME TOPICS



Recall

1st CLASS about Ethical Hacking



Topics

- What is information Gathering/ Footprinting/
- Which information we gather
- Types of information gathering
- How we gather information
- Reverse image search
- Google hacking database

Recon / Information Gathering / Footprint /

- Information Gathering is Collecting data about **some network/host/system.**
- Footprinting => Footstep + printing(logging)
- Most of the people find Footprinting boring, but it is a very important part of Ethical Hacking. Almost 85% of Hacking





Why do we need recon?

- Imagine, You are going to rob a bank... what do you do?
 - Know How much polices are there in the bank
 - Know the doors (way in and out)
 - Know if there is cctv
 - Know which person is the CEO
 - Know which time is Good for robbery
- To Get access on system 1st you have to know the system.
- Knowing the system will lead you to know if the system is vulnerable



Types of information gathering

- **Based on how we do the recon**
 - 1) **Active Footprinting**
 - 2) **Passive Footprinting**



1. Active Footprinting

This kind is when we try to gather information directly by contacting that person.

Example:

- When you go to the bank and ask for some informations.
- Chatting with person on social media to know about them.

Doing Active Footprinting without permission is **ILLEGAL!!**



2. Passive Footprinting

- This kind of recon is when you gather informations from another person,3rd party or by checking public sources.
- Example:
 - To know the bank working time i can see the posted texts.
 - To know someone name by reading the username.



What type of information do you gather?

- We gather information for different things
 - a. Host
 - Websites
 - Computers
 - Smart Phone
 - b. Network
 - Home Network
 - Company networks
 - c. Person/Organization
 - d. Application



How do we gather information?

- Gathering info is classified as we saw early.
- There for the techniques and methods we use can be little different.
- Let us see 1 by one



A. Websites

- The informations we gather about a websites are
 - IP Addresses
 - Development frameworks
 - Technologies used and versions
 - Name
 - DNS informations
 - Subdomains, Assets, Contents



To get ip

- To get ip address of some website:
 - Active recon
 - ping <website link>
 - nslookup <website link>
 - host <website link>
 - Passive recon
 - www.nslookup.io

```
rexder@HunterMachine ~> ping insa.gov.et
PING insa.gov.et (196.188.171.243) 56(84) bytes of data.
^C
--- insa.gov.et ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5237ms
```

```

rexder@HunterMachine ~ [1]> ping facebook.com
PING facebook.com (157.240.201.35) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-ams4.facebook.com (157.240.201.35): icmp_seq=1 ttl=55 t
64 bytes from edge-star-mini-shv-01-ams4.facebook.com (157.240.201.35): icmp_seq=2 ttl=55 t
64 bytes from edge-star-mini-shv-01-ams4.facebook.com (157.240.201.35): icmp_seq=3 ttl=55 t
64 bytes from edge-star-mini-shv-01-ams4.facebook.com (157.240.201.35): icmp_seq=4 ttl=55 t
64 bytes from edge-star-mini-shv-01-ams4.facebook.com (157.240.201.35): icmp_seq=5 ttl=55 t
64 bytes from edge-star-mini-shv-01-ams4.facebook.com (157.240.201.35): icmp_seq=6 ttl=55 t
64 bytes from edge-star-mini-shv-01-ams4.facebook
64 bytes from edge-star-mini-shv-01-ams4.facebook
64 bytes from edge-star-mini-shv-01-ams4.facebook
64 bytes from edge-star-mini-shv-01-ams4.facebook
64 bytes from edge-star-mini-shv-01-ams4.facebook
host google.com
google.com has address 216.58.208.238
google.com has IPv6 address 2a00:1450:4019:805::200e
google.com mail is handled by 10 smtp.google.com.

```

```
rexder@HunterMachine ~> nslookup facebook.com
Server:      172.25.64.1
Address:     172.25.64.1#53
```

```
Non-authoritative answer:  
Name:     facebook.com  
Address:  157.240.201.35  
Name:     facebook.com  
Address:  2a03:2880:f145:82:face:b00c:0:25de
```

DON'T ADD THE HTTPS..

demo..

NsLookup.io

Q insa.gov.et

Find IP addresses

Learning Browser extension API

IP addresses for **insa.gov.et**

All DNS records

Our DNS servers responded with these IP addresses when we queried it for the domain insa.gov.et. Some DNS servers may return different IP addresses based on your location.

IP address	Type	Hosted by	Location
> 196.188.171.243	IPv4	🇪🇹 Ethio Telecom	Ethiopia

Question and response

QUESTION

dig @ insa.gov.et. A

ANSWER

insa.gov.et. 3600 A 196.188.171.243

AUTHORITY

ADDITIONAL

. 0 OPT ; payload 1232, xrcode 0, version 0, f: < >

QUESTION

dig @ insa.gov.et. AAAA

ANSWER

AUTHORITY

insa.gov.et. 1800 SOA ns.insa.gov.et. mail.insa.gov.et. 843 28800 3600 60 < >

ADDITIONAL

. 0 OPT ; payload 1232, xrcode 0, version 0, flags 0

Find the IP addresses for another website or domain name

With [website to IP lookup](#), you can find the IP addresses for any domain name or subdomain. When you enter the domain in the input field below, it will show whether or not IP addresses are configured for that domain.

Q insa.gov.et

Find IP addresses



To get development frameworks

Use simple browser extension

- Wapplyzer
- Builtwith

Terminal tool

- whatweb

demo

Google

wapplyzer for firefox

ሁሉም

ሺዲዮዎች

ካርታዎች

ምስሎች

ተጨማሪ

መሣሪያዎች

ወደ 55,500 የሚደርሱ ውጤቶች (0.39 ሴከንድ) << Add Greppler Answer (a)

Wappalyzer is a **browser extension** that **uncovers the technologies** used on websites. It detects content management systems, eCommerce platforms, web servers, JavaScript frameworks, analytics tools and many more.

<https://addons.mozilla.org> > en-GB > firefox > addon > w...

Wappalyzer – Get this Extension for Firefox (en-GB)

ተለይተው ስለቀረቡ ቅንጥቦች • ግብረ መልስ

TECHNOLOGIES

MORE INFO

Export

Analytics	CDN
Google Analytics UA	cdnjs
Security ✓	Cloudflare
HSTS	Advertising
Font scripts ✓	Google AdSense
Font Awesome 4.7.0	JavaScript libraries ✓
Google Font API	jQuery 1.10.0
Miscellaneous ✓	Reverse proxies
HTTP/2	Nginx
Open Graph	UI frameworks ✓
Web servers	Bootstrap 3.3.7
Nginx	

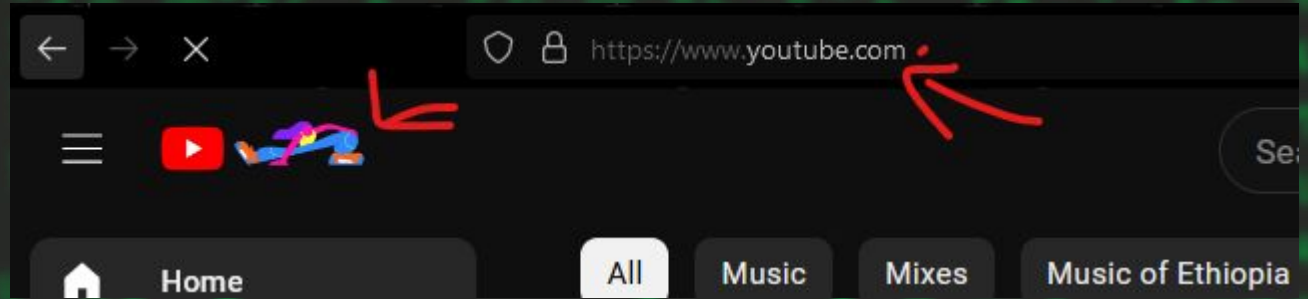
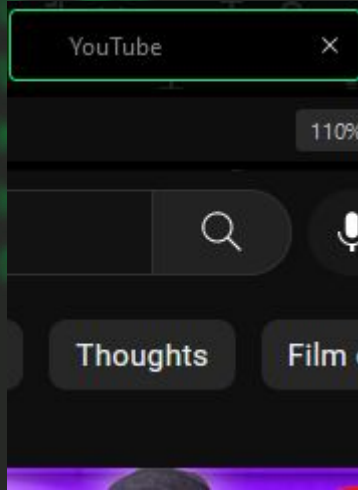
demo...

```
rexder@HunterMachine ~> sudo apt install whatweb
[sudo] password for rexder:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed:
  golang-1.18-go golang-1.18-src pastebinit python3-
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  fonts-lato libgmp-dev libgmp10 libgmpxx4ldbl libru
  ruby-net-telnet ruby-public-suffix ruby-rchardet r
```

```
rexder@HunterMachine ~> whatweb insa.gov.et
http://insa.gov.et [301 Moved Permanently] Apache[2.4.41], HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu
)], IP[196.188.171.243], RedirectLocation[https://insa.gov.et/], Title[301 Moved Permanently]
https://insa.gov.et/ [200 OK] Apache[2.4.41], Bootstrap, Cookies[COOKIE_SUPPORT,GUEST_LANGUAGE_ID,JSESSIO
NID], Email[contact@insa.gov.et], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], HttpOnly[COOKI
E_SUPPORT,GUEST_LANGUAGE_ID,JSESSIONID], IP[196.188.171.243], JQuery, Java, Liferay, Script[text/javascr
ipt], Title[መንግሥት - INSA], UncommonHeaders[x-content-type-options,liferay-portal], X-Frame-Options[SAMEORIG
IN], X-XSS-Protection[1]
```

To get the name

- You can see the title of the website or texts inside the page also the url.



Details about domains

- For this you can use whois terminal + website tool
 - sudo apt install whois
 - whois
 - dig

```
dig google.com

; <<>> DiG 9.19.17-1-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23467
;; flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                0       IN      A      216.58.208.238

;; Query time: 0 msec
;; SERVER: 172.24.64.1#53(172.24.64.1) (UDP)
;; WHEN: Mon Nov 06 19:29:46 EAT 2023
;; MSG SIZE rcvd: 54
```

facebook.com

whois information

Whois

DNS Records

Diagnostics

cache expires in 12 hours, 52 minutes and 42 seconds

[refresh](#)

Registrar Info

Name	RegistrarSafe, LLC
Whois Server	whois.registrarsafe.com
Referral URL	https://www.registrarsafe.com
Status	clientDeleteProhibited https://www.icann.org/epp#clientDeleteProhibited clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited clientUpdateProhibited https://www.icann.org/epp#clientUpdateProhibited serverDeleteProhibited https://www.icann.org/epp#serverDeleteProhibited serverTransferProhibited https://www.icann.org/epp#serverTransferProhibited serverUpdateProhibited https://www.icann.org/epp#serverUpdateProhibited

Important Dates

Expires On	2031-03-30
Registered On	1997-03-29
Updated On	2022-01-26

Name Servers

A.NS.FACEBOOK.COM	129.134.30.12
B.NS.FACEBOOK.COM	129.134.31.12
C.NS.FACEBOOK.COM	185.89.218.12
D.NS.FACEBOOK.COM	185.89.219.12

Similar Domains

[facebook%3Db6ok.com](#) | [facebook-k.com](#) | [facebook-basedbiz.com](#) | [facebook-l.com](#) | [facebook-activate.com](#) | [facebook-color.co.cc](#) | [facebook-design.com](#) | [facebook-error.com](#) | [facebook-junkie.com](#) | [facebook-ok.com](#) | [facebook-ook.com](#) | [facebook-renovation.com](#) | [facebook-server.com](#) | [facebook-survey.com](#) | [facebook.biz](#) | [facebook.br](#) | [facebook.cc](#) | [facebook.chat](#) | [facebook.co](#) | [facebook.co.il](#)



B. Computers/Phone

- The informations we gather about a Computers/Hosts are
 - IP Addresses
 - OS informations
 - HostName
 - MAC address
 - Open services or ports
- Detail on next class



C. Networks

- The informations we gather about a Networks are
 - IP Addresses
 - Ports,Services
 - Class and Type of Network
 - Subnets
 - Hosts on that Network
 - Strength and security of that Network



D. Personal Informations

- The informations we gather about a Persons are
 - Full Name
 - Address
 - Physical Address
 - All Social Media Address
 - Phone address
 - What the person loves
 - Job
 - Friends
 - Status
 - skills
 - ...

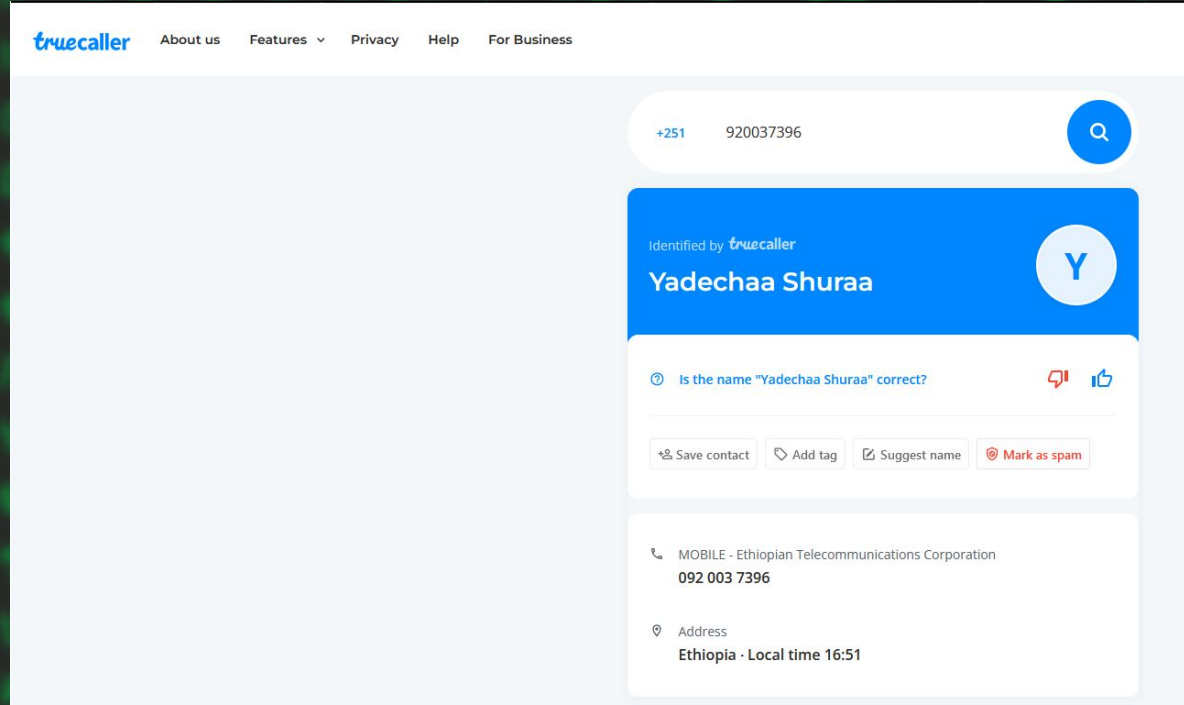


demo...

- Persons information can be gathered by active and passive.
- Gathering and Analyzing Different Informations Based on Public resource is called **OSINT** (Open Source Intelligence)
- There are many methods:...

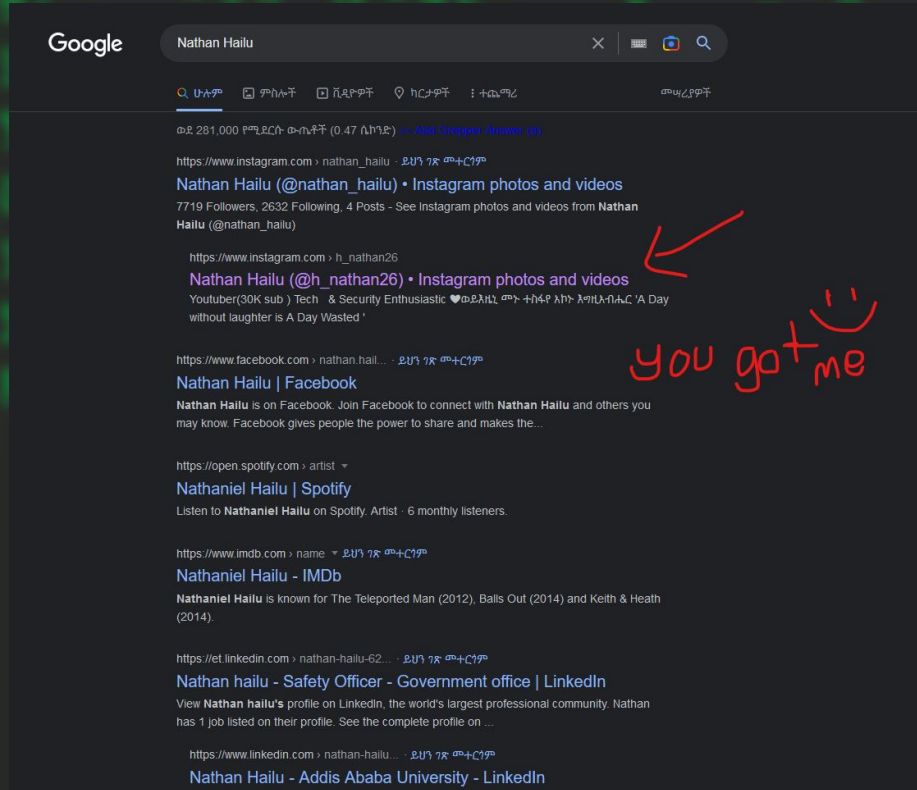
Getting Names by Phone number.

- For this purpose you can use <https://www.truecaller.com/>
- You can get the phone number from social media like telegram, some posted promotion, from websites.



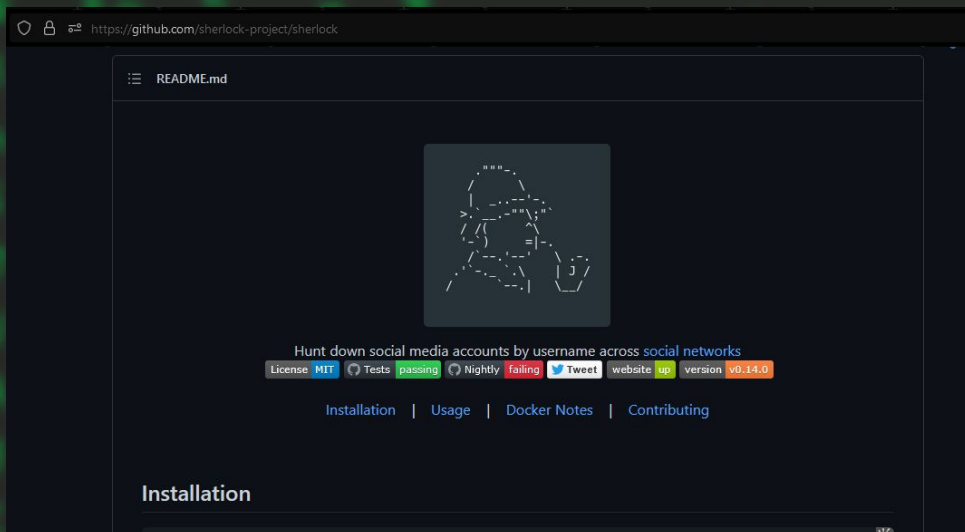
Getting social medias Addresses

- If you have Full name of a person, Just use search engines(google,bing,yahoo)



demo...

Also you can use tool called sherlock from github



```
rexder@HunterMachine ~/t/s/sherlock (master)> python3 sherlock.py nathanhailu
```

```
[*] Checking username nathanhailu on:
```

```
[+] Academia.edu: https://independent.academia.edu/nathanhailu
```

```
[+] Arduino: https://create.arduino.cc/projecthub/nathanhailu
```

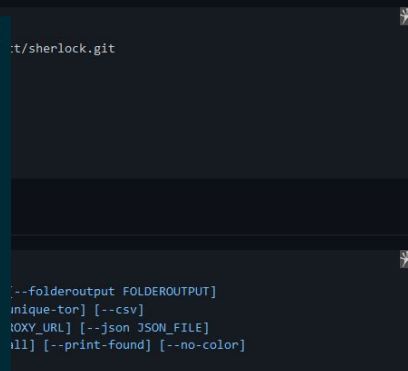
```
[+] Chess: https://www.chess.com/member/nathanhailu
```

```
[+] Clubhouse: https://www.clubhouse.com/@nathanhailu
```

```
[+] Codecademy: https://www.codecademy.com/profiles/nathanhailu
```

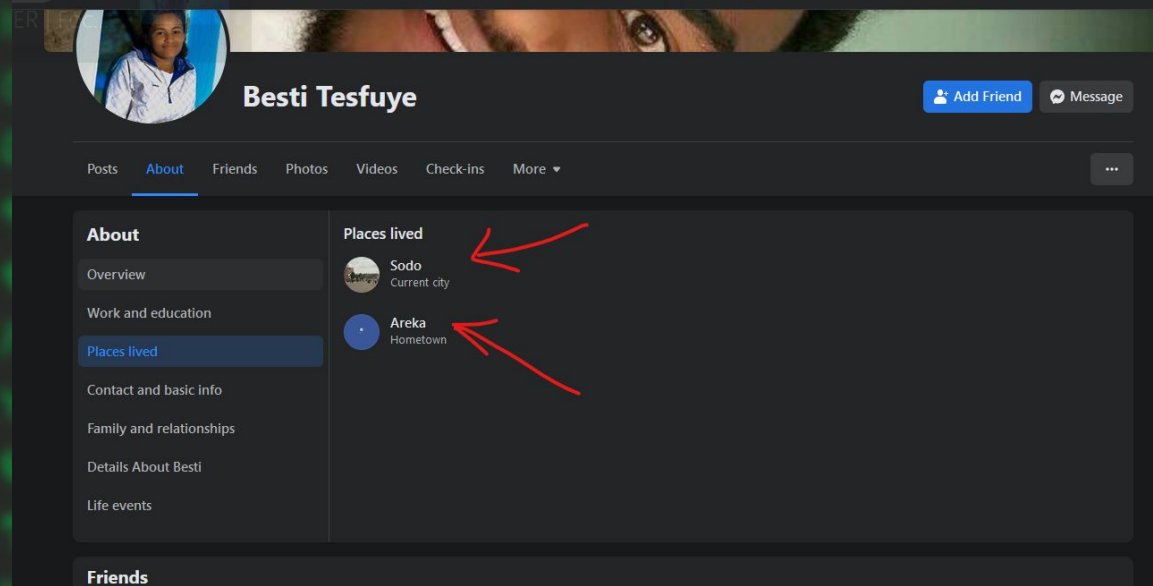
```
[*] Results: 5
```

```
[!] End: The processing has been finished.
```



Getting Physical Addresses

- Peoples share there living place on social medias info page.
- Else there are many methods:
 - Sending links and when people access the link u can get the IP then you can just geolocate the place.



IP geolocation

- If you got the private ip address of someone you can insert it to <https://www.iplocation.net>
- The method of getting the IP might be tricky but detail we will learn on Social Engineering class

Do you have a problem with IP location lookup? Report a problem.

Geolocation data from IP2Location (Product: DB6, 2023-1-1)

IP ADDRESS: 196.188.171.243	ISP: Ethio Telecom
COUNTRY: Ethiopia	ORGANIZATION: Not available
REGION: Addis Ababa	LATITUDE: 9.0250
CITY: Addis Ababa	LONGITUDE: 38.7469

Geolocation data from ipinfo.io (Product: API, real-time)

IP ADDRESS: 196.188.171.243	ISP: Ethio Telecom
COUNTRY: Ethiopia	ORGANIZATION: Ethio Telecom (ethiotelecom.et)
REGION: Addis Ababa	LATITUDE: 9.0250
CITY: Addis Ababa	LONGITUDE: 38.7469

Geolocation data from DB-IP (Product: API, real-time)

IP ADDRESS: 196.188.171.243	ISP: Ethio Telecom
COUNTRY: Ethiopia	ORGANIZATION: Not available
REGION: Addis Ababa	LATITUDE: 9.022
CITY: Addis Ababa	LONGITUDE: 38.7521

Geolocation data from IPRegistry.co (Product: API, real-time)

IP ADDRESS: 196.188.171.243	ISP: Ethio Telecom
COUNTRY: Ethiopia	ORGANIZATION: To Bras Dhcp Oa-10800e (ethiotelecom.et)
REGION: Not available	LATITUDE: 8.99996
CITY: Not available	LONGITUDE: 39.50006

How to know people's behaviour and Obsession

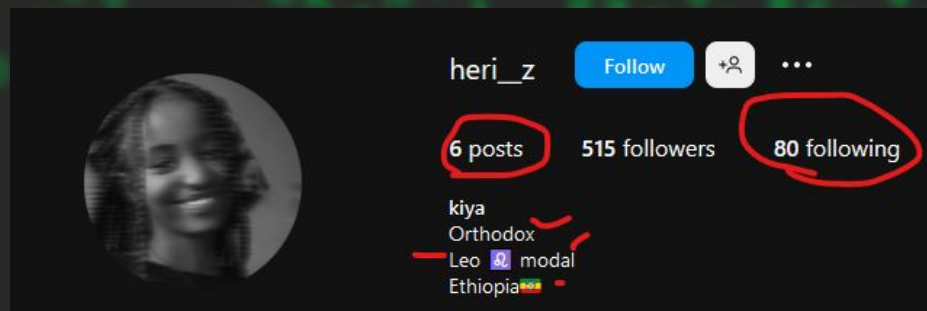
Peoples are being open on social medias, so we Security Testers have access about person behaviours and likes.

Example: instagram is the best place to get info about some user.

Also by seeing telegram Profiles you can get more information about their, religion status, mindset, ideology, family

By checking their followings/friends you can get more common pictures and events, etc....

Detail on Social engineering.





E. Applications/Softwares

- The informations we gather about a Applications are
 - What they are made up of
 - Which programming language used
 - Which framework used
 - Source codes
 - Their logic and Function
 - ...

Exercise 1

15-20min

1. What is the IP Address of <https://moe.gov.et/>
2. What is the IPv6 of <https://google.com/>
3. What is The Full Name of This phone number owner
+251911842577
4. What is the job of user called “Zelalem moges”?
5. What is the Javascript framework of Youtube?





Reverse image search

Reverse image search is a technique of searching with images.

We all search with text but we can search with images to This can give as more information

Ex: think like user posted a picture with a background of some area, if the user didnt talk about the place we can just search the image and the search engines will give as some similar photos where they are taken in same place(not 100% accurate)

We can use:

- <https://tineye.com/>
- <https://www.labnol.org/reverse/>
- <https://images.google.com/>

demo...

Google

በGoogle ሊንክ አማካኝነት ማንኛውንም ምስል ይፈልጉ



ምስል ወደዚህ ይገትቱ ወይም ፋይል ይስቀሩ

ወይም

ምስል አገናኝን ለጥፍ

ፈልግ

Google

ምስል ምንድን አጥኝ



ፍለጋ ድህረ ገጽ ማግኘት

TravKlick



shutterstock.com
60 Gorakh Hill Images,
Stock Photos & Vector...



wallpapercrafter.com
Wallpaper ID: 139162 /
waves, sea, sand,...



wallpapercrafter.com
Wallpaper ID: 139325 /
nature, plants, water,...



lahlanhla.com
LAHLANHLA : Agence
de Voyage Privé Haut...



pibig.info
Бали море - фото и
картинки: 60 штук



youtube.com
Comprehensive Ruqya -
YouTube



worthavegroup.com
Free HD Phone &
Desktop Wallpaper...



lahlanhla.com
LAHLANHLA : Agence
de Voyage Privé Haut...



xfce-look.org
4K Wallpaper The most
wasted of all days is...



facebook.com
Ubuhun Bali | Denpasar



rare-gallery.com
Free Download Beach
wallpaper full hd...



badgermapping.com
40 Motivational &
Inspirational Sales...



shutterstock.com
39 Gorakh Hill Station
Images, Stock Photos ...



andreasara.com
Projects - Andrea Zara



apple.com
Online Wallpaper
Maker: Make your own...



beritagar.id
Bertualang di Bala
Balekang




እነዚህ ውጤቶች ለምሳሌ ሆኑ፡ እንደተጠቀሱት

አዋጅ አይ

demo...


TinEye Search Technology Products About [We are hiring](#)


[Upload](#) Paste or enter image URL


 **4 results**
Searched over 57.7 billion images in 2.3 seconds for:
09addis-national_museum-tewodros02.jpg

☐ Include 1 result not available

Sort by best match Filter by website / collection

 **www.ethiogrio.com**
[movies/20778-agape.html](#) - First found on Feb 18, 2016
[news/index.1.html](#) - First found on Jan 20, 2016
[view all 80 matches](#)
Filename: [thumbnail.php](#) (360 x 246, 11.3 kB)

 **www.ethiogrio.com**
[author/webby/](#) - First found on Jan 24, 2016
[video/talk-shows](#) - First found on Jan 23, 2016
[view all 28 matches](#)
Filename: [thumbnail.php](#) (600 x 410, 22.9 kB)

 **www.elbalad.news**
[www.elbalad.news/](#) - First found on Mar 5, 2019
Filename: [268.jpg](#) (400 x 225, 19.5 kB)



Google Dorking(Google Hacking Database)

- it's not hacking into Google servers!
- Google hacking is using different **Google operators** to effectively optimize search results.
- It also involves using Google to **identify vulnerabilities in websites.**
- Results are **highly customizable.**
- **THIS IS THE MOST POWERFUL SKILL OF HACKER!**



Basic operators

- For inclusion of something common (+)
 - `Nathan Hailu +geeztech +ceo` > don't add space between the sign and the word
- Terms you want to exclude (-)
 - `Antivirus -software`
 - `Georgia -america -state`
- Search for an exact term ("")
 - `"How to eat food"`
 - `"Nathan Hailu"` => what is the difference?



Cont...

- (*) any word (wild card)
 - If you include * within a query, it tells Google to try to treat the star as a placeholder for any unknown term(s) and then find the best matches.

- 

- (|) boolean 'OR'

- 



Advanced Operators

- These are Syntaxes used by Google.
 - intitle
 - Google returns results with the word/phrase found within the title of the page
 - intitle:index.of
 - intitle:"Hackers Bible"
 - inurl
 - Finds a specific term within the URL
 - inurl:view/index.shtml
 - filetype
 - Searches for a specific filetype
 - "Hacking" filetype:pdf
 - filetype:txt
 - Intext
 - Google returns links that contains Texts from that link
 - intext:"Hackers in Ethiopia"

Mixing Operators

`inurl:securethiscompany.com intitle:index.of`

`"mysql dump" inurl: filetype:sql intext:password`

`inurl:ftp "password" filetype:xls`

`intitle:admin intitle:login`

Google

Hacking filetype:pdf

🔍 ሁሉም

📁 ምስሎች


📄 ሽጿዮዎች

📄 መጽሃፍት


⋮ ተጨማሪ

መሠረታዊ

ወደ 24,100,000 የሚደርሱ ውጤቶች (0.51 ሰከንድ) << Add Google Answer (α)


<https://nationalcrimeagency.gov.uk/publications> PDF 
HACKING IT - National Crime Agency


Explain the enjoyable, lucrative and legal options available to them. These include coding, engineering, web development, security operations, law enforcement, ...


<https://nationalcrimeagency.gov.uk/publications> PDF 
HACKING IT - National Crime Agency

The Computer Misuse Act 1990 was introduced into UK Law after two **hackers** obtained, without the persons knowledge, the username and password of an I.T. engineer.

ሰዎች በተጨማሪ ይህን ይጠይቃሉ


What are the 3 types of hacking? 

What hacking meaning? 

What are the 7 types of hackers? 

What are the 4 types of hackers? 

ግብረ መልስ

<https://discovery.ucl.ac.uk/eprint> PDF 

How IT and cybersecurity industry actors perceive good, bad ...

Hacking is part of a larger discourse on and practices around the security of technology, because of **hackers'** tendency to identify, uncover, and exploit ...

25 ገጾች

<https://www.jstor.org/stable>

why "Hacking"? - JSTOR

Hackers are autodidacts. From the earliest **hackers** working at large research universities on the first networks to anyone who deserves the term today, a **hacker** ...



demo

Google

"mysql dump" Inurl: filetype.sql intext:password



🔍 ሁሉም 📄 ሽዲዮዎች 🗂 ምስሎች 🔗 ግጥ ፡ ተጨማሪ መሣሪያዎች

ወደ 191 የሚደርሱ ውሳኔዎች (0.35 ሴከንድ) << [Add Grepper Answer](#) (2)

<http://web.mit.edu> > scripts > textpattern ▾ ይህን ገጽ ሙረገም

web.mit.edu/scripts/deploy/textpattern.sql

MySQL dump 10.9 -- Host: sql.mit.edu Database: presbrey+scriptstp ... 13:39:09')(86,'en-us','change_password','admin','Change your **password**','2005-07-06 ...

<http://www.radiosoft.com> > ext > Database ▾ ይህን ገጽ ሙረገም

www.radiosoft.com/typo3conf/ext/introduction/Resou...

MySQL dump 10.13 Distrib 5.1.57, for apple-darwin11.0.0 (i386) ... timestamp, username, **password**, admin, usergroup, disable, starttime, endtime, lang, email, ...

<http://www.sante.gov.ml> > docs > mysql... ▾ ይህን ገጽ ሙረገም

www.sante.gov.ml/docs/basevida/mysqlbase.sql

... CHARACTER SET latin1 */; USE `mysql`; -- **MySQL dump** 10.13 Distrib 5.6.13, ... such as master host, master port,\nmaster user, and master **password**.

<http://190.0.46.114> > deb1413410033407 ▾ ይህን ገጽ ሙረገም

190.0.46.114/portal/DATOS%20MIGRADOS/deb1413410033...

Adminer 4.2.1 **MySQL dump** SET NAMES utf8; SET time_zone = '+00:00'; SET foreign_key_checks ... '<p>This module displays a username and **password** login form.

<https://github.com> > MPAT-core > blob ▾ ይህን ገጽ ሙረገም

[MPAT-core/dump.sql at master - GitHub](https://github.com/MPAT-core/blob/master/dump.sql)

MySQL dump 10.15 Distrib 10.0.24-MariaDB, for debian-linux-gnu (x86_64) ... with the following information:\n\nUsername: USERNAME\nPassword: **PASSWORD**\nLog ...

<https://github.com> > andalike > mySQL > blob > all_db_b...

[mySQL/all_db_backup.sql at master · andalike/mySQL - GitHub](https://github.com/andalike/mySQL/blob/master/all_db_backup.sql)

MySQL dump 10.13 Distrib 5.7.24, for Linux (x86_64) ... an argument representing a cleartext **password**, this function\nreturns an integer to indicate how ...

demo

Google

intitle:"webcamXP" inurl:8080

🔍 📄 📷 🔍

ወይ 129 የሚደርሱ ውሳኔዎች (0.35 ሰከንድ) <> Add Google Answer (a)

http://109.233.191.130 > ይህን ገጽ መተርጎም

webcamXP 5

webcamXP 5 . webcamXP 5. webcams and ip cameras server for windows.

http://85.93.53.175 > gallery > ይህን ገጽ መተርጎም

webcams and ip cameras server for windows - webcamXP 5

webcamXP 5 . webcamXP 5. webcams and ip cameras server for windows.

http://46.243.108.21 > ይህን ገጽ መተርጎም

webcamXP 5

webcamXP 5 . webcamXP 5. service edition. Home ...

http://67.249.183.177 > frame > ይህን ገጽ መተርጎም

webcamXP 5

http://67.249.183.177 > ይህን ገጽ መተርጎም

webcamXP 5

webcamXP 5 . Inghams Mills Weather. Inghams Mills Weather.

http://et95.no-ip.org > gallery > ይህን ገጽ መተርጎም

webcamXP 5

HomeMulti viewSmartphoneGalleryAdministration. Not logged in. page >> 1 ... 3 4 5 6 7 8 9 10
11 12 13 ... 40. powered by webcamXP 5 v5.9.8.7.

http://99.172.155.145 > ይህን ገጽ መተርጎም

webcamXP 5

YouTube Subscribe JamesJamesNet. YouTube JamesJamesNet. HomeMulti
viewGalleryAdministration. Not logged in. Please provide a valid username/password to ...

http://www.8fincanuckidscenter.com > AMP ምልክት

et95.no-ip.org:8080/gallery.html?page=8

WEBCAMXP 5
WEBCAMS AND IP CAMERAS SERVER FOR WINDOWS

En live, Direction Nord
<http://et95.no-ip.org>
<http://avrfrance.com>

14/05/2017
14:21:02
Connect : 0

T° A jour en fonction du PC
Magny en Vexin (95)
Prévisions météo: ensoleillé

18.2 °C	Temp. E
57 %	Hum. E
9.5 °C	P. de rosée
18.2 °C	Temp au vent
1.5 °C	Indice de chaleur
1022 hPa	P. atm.
dernière Pluie	2 h, 36 min
0.0 mm	Pluie/h
1.0 mm	Pluie/24h
1.448 mm	Ev.Tr.

Captured on 14/05/2017 14:21:02 from source #1

9 of 15

POWERED BY WEBCAMXP 5 V5.9.8.7

html.css



Hackers Power

- Hackers do anything with these operators
- When they Got errors or any problems they use the operators and other.
- Further on google dorking
 - <https://www.exploit-db.com/google-hacking-database>

GHD



Google Hacking Database

Filters Reset All

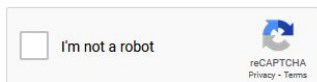
Show 15

Quick Search

Date Added	Dork	Category	Author
2022-09-19	intext:"index of" ".sql"	Files Containing Juicy Info	Gopalsamy Rajendran
2022-09-19	intitle:"index of" inurl:superadmin	Files Containing Juicy Info	Mahedi Hassan
2022-09-19	intitle:"WAMPSEVER Homepage"	Files Containing Juicy Info	HackerFrenzy
2022-09-19	inurl: json beautifier online	Files Containing Juicy Info	Nyein Chan Aung
2022-09-19	intitle:"IIS Windows Server"	Files Containing Juicy Info	HackerFrenzy
2022-09-19	intitle:"index of" inurl:SUID	Files Containing Juicy Info	Mahedi Hassan
2022-09-19	intitle:"index of" intext:"Apache/2.2.3"	Files Containing Juicy Info	Wagner Farias
2022-08-18	inurl:"index.php?page=news.php"	Advisories and Vulnerabilities	Omar Shash
2022-08-18	inurl:/sym404/root	Files Containing Juicy Info	Numen Blog
2022-08-17	inurl:viewer/live/index.html	Various Online Devices	Palvinder Singh Secuneus
2022-08-17	intitle:Index of "venv"	Sensitive Directories	Abhishek Singh
2022-08-17	intitle:"WEB SERVICE" "wan" "lan" "alarm"	Pages Containing Login Portals	Heverin Hacker
2022-08-17	allintitle:"Log on to MACH-ProWeb"	Pages Containing Login Portals	Under The Sea hacker
2022-08-17	intitle:"index of[]"access_token.json"	Files Containing Juicy Info	Leonardo Venegas
2022-08-17	inurl:"admin/default.aspx"	Pages Containing Login Portals	Payal Yedhu

WARNING

If you do a lot of dorkings with same ip address, Google will block you for some hours, and shows you this



About this page

Our systems have detected unusual traffic from your computer network. This page checks to see if it's really you sending the requests, and not a robot. [Why did this happen?](#)

IP address: 149.34.244.178
Time: 2023-01-09T15:25:04Z
URL: https://www.google.com/search?q=%22Nathan+Hailu%22+%2Bgeeztech&newwindow=1&client=firefox-b-d&sxsrf=AJOqlzXHCtRVcEpa62JlcnrABalkEMDtZg%3A1673277431701&ei=9y-8Y_2qKuGX7_UP-Yi90Ag&ved=0ahUKEwi9grWX5Lr8AhXhy7siHXIED4oQ4dUDCA4&uact=5&oq=%22Nathan+Hailu%22+%2Bgeeztech&gs_lcp=Cgxnnd3Mtd2l6LXNlcnAQAzoKCAAQgAQA6BwgAEIAEEBM6CQgAEIAEEA0QEzoCAAQFhAeEBM6BggAEByQhkoECEEYAEoECEEYAFDZB1ibSGCkS2gBcAF4AIABiAylAdl_kgESMC44LjEwLjQuMC4xLjEuMC4xmAEAoAEBByAEIwAEB&client=gws-wiz-serp



Exercise

1. Hey Mr. Hacker give the the pdf file of the stem synergies from insa.gov.et site.
2. What is the text file from insa web-site
 - a. Hint: some files are named in native language
3. Give me screenshot of GHD result of That displays Nathan Hailu with geeztech only



Class is Over!

- 1) DO notes
- 2) Ask questions
- 3) Practice more