

# Bilgi Toplama

---

Necmettin ÇARKACI – Melek Nurten YAVUZ



Biz kimiz

---



# İstihbarat Çeşitleri

---

## Pasif Bilgi Toplama

- Hedef sistemden bağımsız

## Aktif Bilgi Toplama

- Hedef sistemle doğrudan iletişime geçerek



# Pasif Bilgi Toplama

Pasif bilgi toplama, penetrasyon testlerinde bilgi toplama bölümünün ilk adımını teşkil etmektedir. **Hedef sistem ile doğrudan iletişime geçilmez, herhangi bir iz bırakmadan internetin imkanları kullanılarak yapılır.** Hedef ile ilgili tüm bilgiler internet üzerinden kuruma ait sistem ve sunuculara erişmeden toplanmaya çalışılır.



# Pasif Bilgi Toplama

⌚ OSINT (Open Source Intelligence) : Açık istihbarat toplama.



Bilginin değerli olması için illaki gizli olması gerekmiyor.

İstihbarat kaynakları değerli bilgilerin çoğunu açık kaynaklardan elde ediyor.



pipl



## SIK KULLANILAN YÖNTEMLER:

- ⌚ Whois: DNS sorgularını yapabileceğimiz ve pasif bilgi toplamak için kullanılan özel web sayfaları
- ⌚ Arama motorları (Google, Bing, Yahoo vs.)
- ⌚ Sosyal paylaşım ağları (Twitter, Facebook, LinkedIn, Pipl vs.)
- ⌚ Bloglar ve tartışma forumları
- ⌚ Kariyer siteleri
- ⌚ Github



Whois

⌚ Eğer elinizde bir domain varsa `http://www.whois.com.tr/` 'ye girip:

⌚ Bu domain kime ait?

⌚ Hangi sunucu bu web hizmetini sağlıyor?

⌚ Adres ne zaman alındı?

⌚ Nereden satın alındı?

⌚ Şirketin IP aralığı ne, sorumlu yöneticisi kim?

⌚ gibi soruların cevabını bulabilirsiniz.

⌚ Whois komut kullanımı:

⌚ Terminal ekranına **`sudo apt-get install whois`**

⌚ yazarak kurabilir ve **`whois www.blabla.com`** yazarak domain name bilgilerine ulaşabilirsiniz.



# Whois Bilgisi

🕒 whois gtu.edu.tr

```
** Registrant:
GEBZE TEKNİK ÜNİVERSİTESİ REKTÖRLÜĞÜ
GEBZE TEKNİK ÜNİVERSİTESİ REKTÖRLÜĞÜ
PK.141
Kocaeli,
Türkiye
dnsadmin@gyte.edu.tr
+ 90-262-6051000-
+ 90-262-6538490-
```

```
** Administrative Contact:
NIC Handle      : gtu50-metu
Organization Name : Gebze Teknik Üniversitesi Rektörlüğü
Address         : Gebze Teknik Üniversitesi Rektörlüğü
                  P.K 141
                  Kocaeli,41400
                  Türkiye
Phone           : + 90-262-6051000-
Fax             : + 90-262-6538490-
```

```
** Technical Contact:
NIC Handle      : gtu50-metu
Organization Name : Gebze Teknik Üniversitesi Rektörlüğü
Address         : Gebze Teknik Üniversitesi Rektörlüğü
                  P.K 141
                  Kocaeli,41400
                  Türkiye
Phone           : + 90-262-6051000-
Fax             : + 90-262-6538490-
```



# Link Extraction

🕒 lynx -listonly -dump gtu.edu.tr

References

🏠 Home

Desktop

Documents

Downloads

Visible links

1. <http://www.gtu.edu.tr/#content>
2. <http://www.gtu.edu.tr/?languageId=1>
3. <http://www.gtu.edu.tr/kategori/3/3/display.aspx?languageId=1>
4. <http://www.gtu.edu.tr/kategori/2/3/display.aspx?languageId=1>
5. <http://www.gtu.edu.tr/kategori/4/3/display.aspx?languageId=1>
6. <http://www.gtu.edu.tr/kategori/5/3/display.aspx?languageId=1>
7. <http://www.gtu.edu.tr/kategori/6/3/display.aspx?languageId=1>
8. <http://www.gtu.edu.tr/kategori/2280/0/display.aspx>
9. <http://anibal.gyte.edu.tr/portal/>
10. <https://ebys.gtu.edu.tr/enVision/Login.aspx>
11. <http://www.gtu.edu.tr/kategori/2281/0/display.aspx>
12. <http://www.gtu.edu.tr/kategori/975/5/display.aspx?languageId=1>
13. <http://www.gtu.edu.tr/icerik/2140/2699/display.aspx?languageId=1>
14. <http://www.gtu.edu.tr/kategori/1013/3/display.aspx?languageId=1>
15. <http://www.gtu.edu.tr/icerik/972/629/display.aspx?languageId=1>
16. <http://www.gtu.edu.tr/?cl=2>
17. [javascript:;](#)
18. <http://www.gtu.edu.tr/icerik/9/4266/display.aspx?languageId=1>
19. <http://www.gtu.edu.tr/icerik/9/4240/display.aspx?languageId=1>
20. <http://www.gtu.edu.tr/icerik/9/4180/display.aspx?languageId=1>
21. <http://www.gtu.edu.tr/kategori/975/5/display.aspx?languageId=1>



## Ödev :

---

- ⌚ External ve internal linkleri toplayan crawler yazın.
- ⌚ Bulunan alt domainler içindeki linklerde listeye eklensin
- ⌚ Bulunan linkler türüne göre sıralansın.

# ARIN(American Registry for Internet Numbers)

🕒 <https://www.arin.net/> e girip bulduğunuz IP yi arattığınızda IP aralığını i verir.

The screenshot shows the ARIN website's WHOIS-RWS search results. The search was performed for the IP address 50.63.202.28. The results are displayed in a table format, showing the network details and contact information.

**Network**

Net Range	50.62.0.0 - 50.63.255.255
CIDR	50.62.0.0/15
Name	GO-DADDY-COM-LLC
Handle	NET-50-62-0-0-1
Parent	NET50 (NET-50-0-0-0-0)
Net Type	Direct Allocation
Origin AS	AS26496
Organization	GoDaddy.com, LLC (GODAD)
Registration Date	2011-02-02
Last Updated	2014-02-25
Comments	Please send abuse complaints to <a href="mailto:abuse@godaddy.com">abuse@godaddy.com</a>
RESTful Link	<a href="https://whois.arin.net/rest/net/NET-50-62-0-0-1">https://whois.arin.net/rest/net/NET-50-62-0-0-1</a>

**Function**

Function	Point of Contact
NOC	NOC124-ARIN ( <a href="#">NOC124-ARIN</a> )
Tech	NOC124-ARIN ( <a href="#">NOC124-ARIN</a> )


**RELEVANT LINKS**

- > [ARIN Whois/Whois-RWS Terms of Service](#)
- > [Report Whois Inaccuracy](#)
- > [Whois-RWS API documentation](#)
- > [ARIN Technical Discussion Mailing List](#)
- > [Sample stylesheet \(xsl\)](#)




# NETCRAFT

🕒 [http://toolbar.netcraft.com/site\\_report](http://toolbar.netcraft.com/site_report)



Site report for [www.gtu.edu.tr](http://www.gtu.edu.tr)



Netcraft Extension

- Home
- Download Now!
- Report a Phish
- Site Report
- Top Reporters
- Incentives for reporters
- Phishiest TLDs
- Phishiest Countries
- Phishiest Hosters
- Phishiest Certificate Authorities
- Phishing Map
- Takedown Map
- Most Popular Websites
- Branded Extensions
- Tell a Friend

Phishing & Fraud

- Phishing Site Feed
- Hosting Phishing Alerts
- SSL CA Phishing Alerts
- Protection for TLDs against Phishing and Malware
- Deceptive Domain Score
- Bank Fraud Detection
- Phishing Site Countermeasures

Extension Support

- FAQ
- Glossary
- Contact Us
- Report a Bug

Lookup another URL:

Background

Site title	Gebze Teknik Universitesi	Date first seen	March 2015
Site rank		Primary language	Turkish
Description	Büyük Bir Devlet Üniversitesi		
Keywords	Not Present		


Network

Site	<a href="http://www.gtu.edu.tr">http://www.gtu.edu.tr</a>	Netblock Owner	Gebze Yuksek Teknoloji Enstitusu
Domain	<a href="http://gtu.edu.tr">gtu.edu.tr</a>	Nameserver	ns1.gtu.edu.tr
IP address	193.140.134.3	DNS admin	dnsadmin@gtu.edu.tr
IPv6 address	Not Present	Reverse DNS	dyn.gtu.edu.tr
Domain registrar	nic.tr	Nameserver organisation	whois.nic.tr
Organisation	GEBZE TEKNİK ÜNİVERSİTESİ REKTÖRLÜĞÜ	Hosting company	gyte.edu.tr
Top Level Domain	Turkey (.edu.tr)	DNS Security Extensions	unknown
Hosting country	🇹🇷 TR		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen	Ref
<a href="#">Gebze Yuksek Teknoloji Enstitusu</a>	193.140.134.3	Windows Server 2008	Microsoft-IIS/7.5	15-Jun-2016	<a href="#">Ref</a>

Security

Netcraft Risk Rating <a href="#">[FAQ]</a>	1/10 	On Exploits Block List	No
On Spamhaus Block List	No	On Domain Block List	No
On Policy Block List	No		

Sender Policy Framework

# CENTRALOPS:

centralops.net/co/

**Central Ops .net** Advanced online Internet utilities

**Utilities**

- Domain Dossier
- Domain Check
- Email Dossier
- Browser Mirror
- Ping
- Traceroute
- NsLookup
- AutoWhois
- TcpQuery
- AnalyzePath

**Domain Dossier** Investigate domains and IP addresses

domain or IP address

☒ domain whois record ☒ DNS records ☐ traceroute

☒ network whois record ☐ service scan

user: anonymous [85.97.174.44]  
balance: 45 units  
[log in](#) | [account info](#)

**Address lookup**

canonical name [onedio.com.](#)

aliases

addresses 2400:cb00:2048:1::6814:17f7  
2400:cb00:2048:1::6814:18f7  
104.20.23.247  
104.20.24.247

**Domain Whois record**

Queried [whois.internic.net](#) with "dom onedio.com"...

```
Domain Name: ONEDIO.COM
Registrar: NAME.COM, INC.
Sponsoring Registrar IANA ID: 625
Whois Server: whois.name.com
Referral URL: http://www.name.com
Name Server: HEATHER.NS.CLOUDFLARE.COM
Name Server: WOZ.NS.CLOUDFLARE.COM
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Updated Date: 01-apr-2015
Creation Date: 27-nov-2010
Expiration Date: 27-nov-2018

>>> Last update of whois database: Fri, 14 Oct 2016 19:32:19 GMT <<<

For more information on Whois status codes, please visit https://icann.org/epp

Queried whois.name.com with "onedio.com"...
```

```
Domain Name: ONEDIO.COM
Registry Domain ID: 1627560233_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.name.com
Registrar URL: http://www.name.com
Updated Date: 2015-04-01T19:59:07Z
Creation Date: 2010-11-27T15:20:17Z
Registrar Registration Expiration Date: 2018-11-27T15:20:17Z
Registrar: Name.com, Inc.
```



**Utilities**

Domain Dossier  
Domain Check  
Email Dossier  
Browser Mirror

Ping  
Traceroute  
Nslookup  
AutoWhois  
TcpQuery  
AnalyzePath


```
Registrar Name: O.S.T.  
Reseller:  
Domain Status: clientTransferProhibited  
Registry Registrant ID:  
Registrant Name: Onedio Bilisim  
Registrant Organization: Onedio Bilisim Yazilim Medya Tekn. San. Tic. A.S  
Registrant Street: ODTU Teknokent Silikon Blok No:35  
Registrant City: Ankara  
Registrant State/Province: Cankaya  
Registrant Postal Code: 06060  
Registrant Country: TR  
Registrant Phone: +90.3122101048  
Registrant Email: onediocom@gmail.com  
Registry Admin ID:  
Admin Name: Arsen Nurmagomedov  
Admin Organization: Onedio Bilisim Yazilim Medya Tekn. San. Tic. A.S  
Admin Street: ODTU Teknokent Silikon Blok No:35  
Admin City: Ankara  
Admin State/Province: Cankaya  
Admin Postal Code: 06060  
Admin Country: TR  
Admin Phone: +90.5301040767  
Admin Email: arsen@onedio.com  
Registry Tech ID:  
Tech Name: Ekin Koc  
Tech Organization: Onedio Bilisim Yazilim Medya Tekn. San. Tic. A.S  
Tech Street: ODTU Teknokent Silikon Blok No:35  
Tech City: Ankara  
Tech State/Province: Cankaya  
Tech Postal Code: 06060  
Tech Country: TR  
Tech Phone: +90.5327980532  
Tech Email: ekin@onedio.com  
Name Server: woz.ns.cloudflare.com  
Name Server: heather.ns.cloudflare.com  
DNSSEC: Unsigned Delegation  
Registrar Abuse Contact Email: abuse@name.com  
Registrar Abuse Contact Phone: +1 7203101849  
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/  
>>> Last update of WHOIS database: 2016-10-14T13:32:29-06:00 <<<
```

**Network Whois record**

Queried **whois.arin.net** with "n 104.20.23.247"...

```
NetRange:      104.16.0.0 - 104.31.255.255  
CIDR:          104.16.0.0/12  
NetName:       CLOUDFLARENET  
NetHandle:     NET-104-16-0-0-1  
Parent:        NET104 (NET-104-0-0-0-0)  
NetType:       Direct Assignment  
OriginAS:      AS13335  
Organization:  CloudFlare, Inc. (CLOUD14)  
RegDate:       2014-03-28  
Updated:       2015-10-01
```

# IPAddress.com

 **IPAddress.com**  
The Best IP Address Tools

My IP | IP Tools | Email Tools | Speed Test | Articles

My IP: 85.97.174.44

Search for a IP Address, Domain or Hostname


## Onedio.com

Onedio Website and Webhosting Information

### Advertisements

We found that the organization hosting Onedio.com is CloudFlare in San Francisco, California, United States.

A more detailed IP address report for Onedio.com is below. At the time you pulled this report, the IP of Onedio.com is 104.20.23.247 and is located in the time zone of America/Los\_Angeles. The context of Onedio.com is "Onedio" and could reflect the theme of the content available on the resource. More IP details of Onedio.com are shown below along with a map location.

IP Address of Onedio is 104.20.23.247			
Hostname:	onedio.com	City:	San Francisco
IP Address:	104.20.23.247	Country:	United States 
Organization:	CloudFlare	State:	California
ISP/Hosting:	CloudFlare	Postal Code:	94107
Updated:	10/09/2016 09:06 PM	Timezone:	America/Los_Angeles
		Local Time:	10/14/2016 12:41 PM

[Top of the page](#)


### Onedio.com Reverse IP | Websites on the same Webhosting

We found 1 hostname for IP Address 104.20.23.247

1	onedio.com
---	------------

[Top of the page](#)

### Map location for Onedio.com | Onedio



onedio.com.ipaddress.com

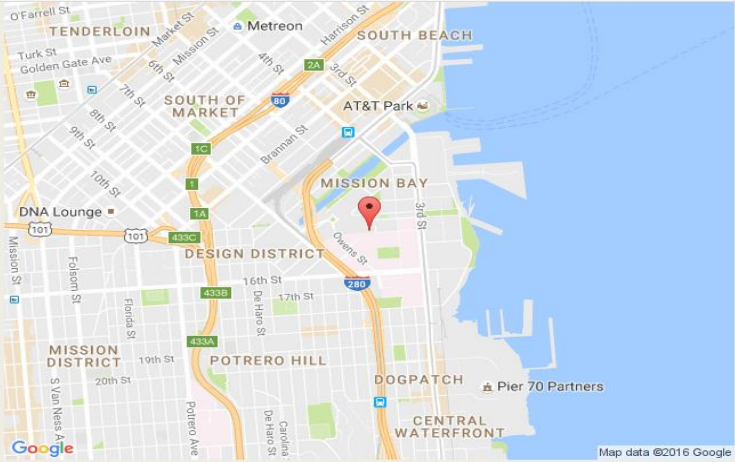
IPAddress.com  
The Best IP Address Tools

My IP IP Tools Email Tools Speed Test Articles

My IP: 85.97.174.44

Search for a IP Address, Domain or Hostname

### Map location for Onedio.com | Onedio



Map data ©2016 Google

Top of the page

### Onedio.com Whois

Registrar	Name.com, Inc.
Whois Server	whois.name.com
Referral URL	http://www.name.com



# Wayback Machine

🕒 1966 dan bu yana web sitelerin önceki kaydedilmiş bilgilerini tutar.



# Waybackmachine



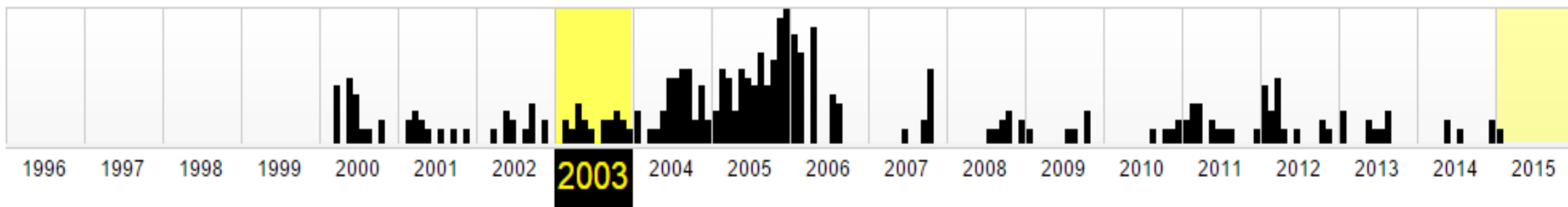
<http://www.mynet.com.tr>

BROWSE HISTORY

<http://www.mynet.com.tr>

Saved **474 times** between Mart 1, 2000 and Ocak 1, 2015.

**PLEASE DONATE TODAY.** Your generosity preserves knowledge for future generations. Thank you.








# Facebook

- Anne kızlık soyadı
- Doğum tarihi
- En sevdiği film
- En sevdiği renk
- Tuttuğu takım



# Pipl.com


→  Pipl, Inc [US] | <https://pipl.com/search?q=halil+öztürkçi&l=8&loc=8&in=6>

Search By

First

Last

+ MORE OPTIONS 


☒ All Locations


☐ Turkey



☐ Istanbul


☐ United States


Results for **Halil Öztürkçi**



 **Halil Ozturkci**  
Istanbul, Turkey  
SPONSORED: [Contact Details](#) | [Username Report](#)  
Partner at ADEO IT Consulting Services and 3 more jobs

 **Halil Öztürkci**  
Istanbul, Turkey  
SPONSORED: [Social Profile](#) | [Username Report](#)  
Known online as halilozturkci

 **Halil Öztürkci, halilozturkci**  
[soundcloud.com/halilozturkci](https://soundcloud.com/halilozturkci)  
 Member's Profile - SoundCloud

 **Halil Öztürkci**  
Associated with Uğur Güngör  
SPONSORED: [Vital Records](#) | [Contact Details](#)

 **Halil Öztürkci**  
Istanbul, Turkey  
SPONSORED: [Contact Details](#)

 **Halil Öztürkci, halil.ozturkci**  
[facebook.com/people/\\_/100003080037125](https://facebook.com/people/_/100003080037125)  
 Personal Web Profile - Facebook



İş ilanları - Kariyer.net

---



linkedin

---



Haberler

---



# Theharvester Script

```
root@kali:~# theharvester
```

```
*****
*
* | | | | _ _ _ _ ^ ^ _ _ _ _ _ _ _ _ | | _ _ _ _ _ _ _ _
* | | | ' _ _ / _ _ / _ _ / _ _ / _ _ / _ _ / _ _ / _ _
* | | | | | _ _ / _ _ / ( | | | _ _ v / _ _ ^ _ _ | | _ _ /
* \ _ _ | | \ _ _ | \ / _ _ \ _ _ , _ _ | \ / \ _ _ | | _ _ ^ \ _ _ | |
*
* TheHarvester Ver. 2.2a
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****
```

Usage: theharvester options

- d: Domain to search or company name
- b: Data source (google,bing,bingapi,pgp,linkedin,google-profiles,people123,jigsaw,all)
- s: Start in result number X (default 0)
- v: Verify host name via dns resolution and search for virtual hosts
- f: Save the results into an HTML and XML file
- n: Perform a DNS reverse query on all ranges discovered
- c: Perform a DNS brute force for the domain name
- t: Perform a DNS TLD expansion discovery
- e: Use this DNS server
- l: Limit the number of results to work with(bing goes from 50 to 50 results,
- h: use SHODAN database to query discovered hosts  
google 100 to 100, and pgp doesn't use this option)

Examples: theharvester -d microsoft.com -l 500 -b google  
          theharvester -d microsoft.com -b pgp  
          theharvester -d microsoft -l 200 -b linkedin



# Theharvester Script

---

⌚ root@kali:~# theharvester -d kali.org -l 500 -b Google

⌚ root@kali:~# theharvester -d kali.org -l 200 -b linkedin

⌚ root@kali:~# theharvester -d kali.org -l 500 -b all



# Discover Script

---

- ⌚ <https://github.com/leeбайд/discover> adresinden indirip kurun.
- ⌚ ./discover.sh
- ⌚ 1 domain için
- ⌚ 1 pasif tarama
- ⌚ gtu.edu.tr taranacak adres
- ⌚ /root/result.html sonuçları çıktı olarak al





# Google Hacking Database (GHDB)



[Home](#) [Exploits](#) [Shellcode](#) [Papers](#) [Google Hacking Database](#) [Submit](#) [Search](#)

## Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Any Category ▼

Search

SEARCH

Date	Title	Category
2016-08-16	inurl:/Portal/Portal.mwsl	Various Online Devices
2016-08-16	intitle:"bandwidthd" "programmed by david hinkle, commissioned by derbytech wireless networking."	Network or vulnerability data
2016-08-16	inurl:index of driver.php?id=	Error Messages
2016-08-08	inurl:/FCKeditor/editor/filemanager/upload/	Sensitive Directories
2016-08-05	inurl:Dialin/Conference.aspx	Pages containing login portals
2016-07-27	inurl:pictures intitle:index.of	Sensitive Directories
2016-07-25	inurl:sgms/auth	Advisories and Vulnerabilities
2016-07-20	site:static.ow.ly/docs/ intext:@gmail.com   Password	Files containing passwords
2016-07-15	inurl:DiGIR.php	Files containing juicy info
2016-07-07	filetype:sql intext:wp_users phpmyadmin	Files containing juicy info





# Google Hacking Database (GHDB)

Özellik	Komut	Örnek
Url arama	inurl	hostname:"google"
Başlıkta arama	intitle	port:"21"
Dosya tipinde arama	filetype	country:"United States"
City	intext	city:"New York"
Organization/Company	author	org:"Amazon"
Internet Service Provider	site	isp:"Hostwinds LLC"
OS/Product/Platform	link	product:"Apache httpd"
Product Version	datarange	version:"2.2.15"
Geo Location	numrange	geo:"39.6949,-83.1383"
Date	insubject	before:"12-12-15"
IP Address/Subnet	msgid	net:"74.91.246.0/24"





# Google Hacking Database (GHDB)

---

- ① [inurl:private\\_files](#) özel klasörler
- ① [site:https://github.com/inurl:.ssh/id\\_rsa](#) github adresinde bulunan private keyler
- ① ["BEGIN RSA PRIVATE KEY" filetype:key -github](#)





# Google Hacking Database (GHDB)

---

- ⌚ Kategoriler :
- ⌚ [Files Containing Juicy Info](#)
- ⌚ [Files Containing Passwords](#)
- ⌚ [Sensitive Online Shopping Info](#)
- ⌚ [Network or Vulnerability Data](#)
- ⌚ [Vulnerable Servers](#)



## SiteDigger :

- ⌚ Google 'ın arama tekniklerini kullanan ve Google 'ın ön belleğinde bulunan sayfalarda yukarıdaki bilgi toplama tekniklerini ve sayfa üzerindeki zafiyetleri raporlayan SiteDigger aracı **pasif bilgi toplamada** kullanılması gereken araçlardandır.

⌚ Google ve Google için yazılmış pasif bilgi toplama araçlarını kullanarak kuruma ait kritik bilgiler, mail adresleri, veritabanı dosyaları, yönetici erişimleri ve daha bir çok bilgi elde edilebilir. Elde edilen bilgiler penetrasyon testinin diğer aşamaları için ciddi değer ve önem taşır.

⌚ Linkten indirebilirsiniz:

<http://www.mcafee.com/us/downloads/free-tools/sitedigger.aspx#>



- FSDB(175)
- Backup Files(12)
- Configuration Manage
- Error Messages(39)
- Privacy Related(30)
- Remote Administration
- Reported Vulnerabilit
- Technology Profile(43)
- "# Dumping data
- "# phpMyAdmin M
- "# phpMyAdmin M
- "#mysql dump" fil
- "cacheserverrepo
- "Host Vulnerability
- "Index of" / "chal
- "Most Submitted I
- "Network Host As
- "Network Vulnera
- "phpinfo.php" -ma
- "robots.txt" + "Dis
- "Select a databas
- "Thank you for yo
- "These statistics v
- "This file was gen
- "This report lists"
- "This report was g
- "This summary wa
- "Welcome to PHF
- "YaBB SE Dev To
- filetype.htaccess l
- intitle:"Ganglia" "
- intitle:"Index of" "
- intitle:"Index of" m
- intitle:"Index of" s
- intitle:"vbm" con
- intitle:admin intitle
- intitle:Index of rob
- intitle:Index of "Ap
- intitle:Index of cgi
- intitle:Index of hac

Site/Domain:  [Optional]

Cancel

Clear

Queries Scanned:

Selected Entry Info:

161 intitle:index.of robots.txt F95  
162 intitle:index.of "Apache" "server at" F75  
163 intitle:index.of cgiirc.config' F64  
164 intitle:index.of haccess.cgi F69  
165 intitle:index.of master.passwd F23  
166 inurl:admin intitle:login F82  
167 inurl:'cgiirc.config' F65  
168 inurl:change-password.asp F83  
169 inurl:ipsec.conf -intitle:manpage F87  
170 inurl:ipsec.secrets "holds shared secrets" F89  
171 inurl:ipsec.secrets -history -bugs F88  
172 inurl:main.php phpMyAdmin F84

Scanning...


Results: [Double click a link to open in default browser]

URL	Query	Category



# Shodan.io Üzerinden Bilgi Toplama

[Shodan](#) [Scanhub](#) [Developers](#) [View All...](#)

 **SHODAN**

**Shodan**  
World's first search engine for the Internet of Things.


**Maps**  
Intuitive map interface to search the Shodan database.


**Images**  
A stream of screenshots from crawled devices.


**Exploits**  
Search across a variety of vulnerability databases at once.


**Scanhub**  
Make your Nmap results searchable by uploading them to Scanhub.


**Blog**  
Stay up to date with the latest developments and research.

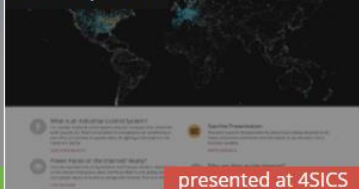
**My Account**  



**Developer API**  


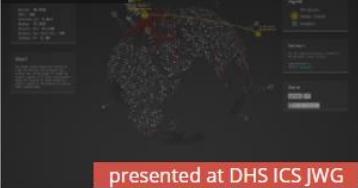
**Maltego Add-On**  



**Chrome Browser Plugin**  



**Firefox Plugin**  



**3rd party**  



**Webcam Browser**  


**ICS Radar**  
  
presented at DHS ICS JWG

**Shodan CLI**  


**Map of the Internet**  


**Honeypot Or Not**  
  
presented at Kaspersky SAS

**Shodan 3D**  
  
presented at 4SICS


**Shodan**, çevrimiçi bulunan belirli cihazları ve cihaz türlerini bulmak için kullanılan bir arama motorudur. En popüler aramalar web kamerası, linksys, cisco, netgear, SCADA vb. içindir.





# Shodan.io Üzerinden Bilgi Toplama

[Shodan](#) [Developers](#) [Book](#) [View All...](#)


 **SHODAN**


[Explore](#) [Downloads](#) [Reports](#) [Enterprise Access](#) [Contact Us](#) [My Account](#)

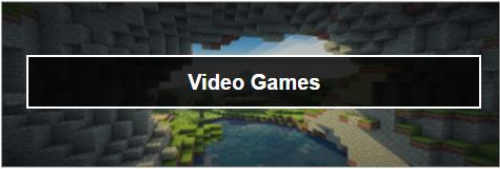
## Explore

Discover the Internet using search queries shared by other users.

### Featured Categories

**Industrial Control Systems**

**Databases**

**Video Games**

### Top Voted

7,414

**Webcam**  
best ip cam search I have found yet.

[webcam](#) [surveillance](#) [cams](#)

2010-03-15

2,620

**Cams**  
admin admin

[cam](#) [webcam](#)

2012-02-06

1,664

**Netcam**  
Netcam

[netcam](#)

2012-01-13

### Recently Shared

1

**webcam**  
webcam

2016-08-16

2

**matrimonio**

2016-08-15

1

**X-Pingback wordpress Denial of service**  
kelvinsecurity



2016-08-15






# Shodan.io Üzerinden Bilgi Toplama

[Shodan](#) [Developers](#) [Book](#) [View All...](#)

 **SHODAN**   [Explore](#) [Downloads](#) [Reports](#) [Enterprise Access](#) [Contact Us](#)

[Exploits](#) [Maps](#) [Share Search](#) [Create Report](#)

### TOP COUNTRIES



Turkey	80
--------	----

### TOP CITIES

Istanbul	10
Ankara	6
Kocaeli	3
Sanayi	2
Mugla	1

### TOP SERVICES

Telnet	48
HTTP	13
8081	6
8880	2
GlassFish Server	2

### TOP ORGANIZATIONS


Turk Telekom	40
Vodafone Net İletişim Hizmetleri A.Ş.	12
Tellcom İletişim Hizmetleri A.Ş.	4
TurkNet İletişim Hizmetleri A.Ş.	3
Vodafone Turkey 3G IP Pool	2

### TOP PRODUCTS

nginx	7
TP-LINK WR841N WAP http config	1
TP-LINK WR740N WAP http config	1
Microsoft IIS httpd	1


Total results: 79

## 213.254.131.44

**Tellcom İletişim Hizmetleri A.Ş.**  
Added on 2016-11-20 10:55:23 GMT  
 Turkey  
[Details](#)


HTTP/1.1 200 OK  
Server: nginx  
Date: Sun, 20 Nov 2016 10:55:22 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Connection: keep-alive  
Keep-Alive: timeout=20  
Set-Cookie: iMSCP\_Session=4ucncophigkb53v2dkbh48scd0; path=/  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: ...

## 46.197.117.21

**mail.bioartmed.com**  
**Turksat Uydu-Net Internet**  
Added on 2016-11-20 07:14:29 GMT  
 Turkey  
[Details](#)

HTTP/1.1 200 OK  
Server: nginx  
Date: Sun, 20 Nov 2016 07:14:06 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Connection: keep-alive  
Last-Modified: Sun, 20 Nov 2016 07:14:05 GMT  
X-Frame-Options: SAMEORIGIN  
Set-Cookie: PHPSESSID=7h381j0utqmtffv3co32ivc1tph2ojms; path=...

## 78.186.175.34

**78.186.175.34.static.ttnet.com.tr**  
**Turk Telekom**  
Added on 2016-11-20 07:13:45 GMT  
 Turkey, Kocaeli  
[Details](#)


<HTML>  
<HEAD>  
<META http-equiv="Pragma" content="no-cache">  
<META http-equiv="Content-Type" content="text/html; charset=utf-8">  
<title>Tenda ADSL2/2+ Modem with Wireless Router</title>  
  
<script language="javascript" src="translate.js"></script>  
<SCRIPT language=JavaScript>  
TranslateDictio...

Shodan


Developers

Book

View All...

 SHODAN

default password country:tr




Explore


Downloads


Reports


Enterprise Access

Contact Us


 Exploits

 Maps

 Share Search

 Create Report

TOP COUNTRIES



|        |    |
|--------|----|
| Turkey | 80 |
|--------|----|

TOP CITIES

|          |    |
|----------|----|
| Istanbul | 10 |
| Ankara   | 6  |
| Kocaeli  | 3  |
| Sanayi   | 2  |
| Mugla    | 1  |

TOP SERVICES

|                  |    |
|------------------|----|
| Telnet           | 48 |
| HTTP             | 13 |
| 8081             | 6  |
| 8880             | 2  |
| GlassFish Server | 2  |

TOP ORGANIZATIONS

|                                      |    |
|--------------------------------------|----|
| Turk Telekom                         | 40 |
| Vodafone Net Iletisim Hizmetleri A.s | 12 |
| Tellcom Iletisim Hizmetleri A.s.     | 4  |
| TurkNet Iletisim Hizmetleri A.S      | 3  |
| Vodafone Turkey 3G IP Pool           | 2  |

TOP PRODUCTS


|                                |   |
|--------------------------------|---|
| nginx                          | 7 |
| TP-LINK WR841N WAP http config | 1 |
| TP-LINK WR740N WAP http config | 1 |
| Microsoft IIS httpd            | 1 |

Total results: 79

213.254.131.44

Tellcom Iletisim Hizmetleri A.s.

Added on 2016-11-20 10:55:23 GMT

 Turkey

Details

HTTP/1.1 200 OK

Server: nginx

Date: Sun, 20 Nov 2016 10:55:22 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

Keep-Alive: timeout=20

Set-Cookie: IMSCP\_Session=4ucncohpigkb53v2dkbh48scd0; path=

Expires: Thu, 19 Nov 1981 08:52:00 GMT


Cache-Control: no-cache

46.197.117.21

mail.bioartmed.com

Turksat Uydu-Net Internet

Added on 2016-11-20 07:14:29 GMT

 Turkey

Details

HTTP/1.1 200 OK

Server: nginx

Date: Sun, 20 Nov 2016 07:14:06 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

Last-Modified: Sun, 20 Nov 2016 07:14:05 GMT

X-Frame-Options: SAMEORIGIN


Set-Cookie: PHPSESSID=7h381j0utqmtffv3co32ivc1tph2ojms; path=...

78.186.175.34

78.186.175.34.static.ttnet.com.tr

Turk Telekom

Added on 2016-11-20 07:13:45 GMT

 Turkey, Kocaeli

Details

<HTML>

<HEAD>

<META http-equiv="Pragma" content="no-cache">

<META http-equiv="Content-Type" content="text/html; charset=utf-8">

<title>Tenda ADSL2/2+ Modem with Wireless Router</title>

<script language="javascript" src="translate.js"></script>

<SCRIPT language=JavaScript>

TranslateDictio...



# Shodan.io parametreler

| Özellik                   | Komut        | Örnek                   |
|---------------------------|--------------|-------------------------|
| Host/Domain               | hostname     | hostname:"google"       |
| Port/Service              | port         | port:"21"               |
| Country                   | country      | country:"United States" |
| City                      | city         | city:"New York"         |
| Organization/Company      | org          | org:"Amazon"            |
| Internet Service Provider | isp          | isp:"Hostwinds LLC"     |
| OS/Product/Platform       | product      | product:"Apache httpd"  |
| Product Version           | version      | version:"2.2.15"        |
| Geo Location              | geo          | geo:"39.6949,-83.1383"  |
| Date                      | before/after | before:"12-12-15"       |
| IP Address/Subnet         | net          | net:"74.91.246.0/24"    |



# Uygulama - Shodan.io

---

- ⌚ Markalara göre ürünlerin varsayılan şifreleri:  
<http://www.phenoelit.org/dpl/dpl.html>
- ⌚ linux upnp avtech country:tr city:İstanbul (Ip kameralar)
- ⌚ country:tr port:3389 (Mysql veritabanları))
- ⌚ country:tr port:21 "Anonymous access granted" (Anonim ftp hesapları)  
â [ftp://85.105.213.197/Matica/ROKETSAN\\_20160811/](ftp://85.105.213.197/Matica/ROKETSAN_20160811/)





# Metadata Analiz Aracı

Microsoft - FOCA Free 2.6

File Metadata Domain Enumeration Software Recognition Tools Logs Options About

Network data Metadata

Documents (0/248)  
Metadata Summary  
Users  
Folders  
Printers  
Software  
Emails  
Operating Systems

**Download the New**  
**FOCA 2.6**  
-DNS Snooping  
-Fingerprinting  
-HTTP Methods  
-...and more

**Search engines**  
☒ Google  
☒ Bing  
☒ Exalead

**Extensions**  
☒ doc ☒ pptx ☒ sxi ☒ pdf  
☒ ppt ☒ ppsx ☒ odt ☒ wpd  
☒ pps ☒ xlsx ☒ ods ☒ svg  
☒ xls ☒ sxw ☒ odg ☒ svgz  
☒ docx ☒ sxc ☒ odp ☒ indd

[Custom search](#) Search All

| Id | Type | URL  | Download |
|----|------|--|----------|
| 0  | doc  | http://www.microsoft.com/korea/sharepoint/techinfo/development/BuildCorpPortalusingXP_kr.doc | ×        |
| 1  | doc  | http://www.microsoft.com/southafrica/partner/2002_exams.doc                                  | ×        |
| 2  | doc  | http://www.microsoft.com/exchange/evaluation/tiwin2003.doc                                   | ×        |
| 3  | doc  | http://www.microsoft.com/usability/UEPostings/DesirabilityToolkit.doc                        | ×        |
| 4  | doc  | http://www.microsoft.com/usability/UEPostings/ProductReactionCards.doc                       | ×        |
| 5  | doc  | http://www.microsoft.com/office/dataanalyzer/evaluation/DAGuide.doc                          | ×        |
| 6  | doc  | http://www.microsoft.com/Spain/HomePage/PosturaUE.doc  | ×        |
| 7  | doc  | http://www.microsoft.com/Presspass/presskits/dynamics/docs/conv11/0412sonata.doc             | ×        |
| 8  | doc  | http://www.microsoft.com/exchange/evaluation/overview/ECSReleaseNotes.doc                    | ×        |
| 9  | doc  | http://www.microsoft.com/taiwan/business/licensing/Software_Assurance_Briefing.doc           | ×        |
| 10 | doc  | http://www.microsoft.com/biztalk/techinfo/biztalkframework20.doc                             | ×        |
| 11 | doc  | http://www.microsoft.com/business/downloads/health/enhancingpsq.doc                          | ×        |
| 12 | doc  | http://www.microsoft.com/exchange/evaluation/ti/tiwin2003.doc                                | ×        |
| 13 | doc  | http://www.microsoft.com/investor/reports/ar09/downloads/MS_2009_AR.doc                      | ×        |
| 14 | doc  | http://www.microsoft.com/colombia/socios/downs/GuideLicenciamientoparaSocios.doc             | ×        |
| 15 | doc  | http://www.microsoft.com/usability/UEPostings/HCI-kirstenrisden.doc                          | ×        |
| 16 | doc  | http://www.microsoft.com/solutions/edi/download/na/BOM_Request_EBISXML_10.doc                | ×        |

Search stopped





# Metadata Analiz Aracı

---

- ⌚ Windows ortamında çalışıyor.
- ⌚ Online ortamda ilgili adrese ait dosyaları toplayıp metada datalarını analiz ediyor.
- ⌚ Metada bilgisi üzerinde sisteme ait bilgi üretiyor.



Diğerleri

---



# Aktif Bilgi Toplama



# Kaynakça

---