



Welcome to
Cyber Security Training

Footprinting Concepts

Objectives of Footprinting

The major objectives of Footprinting are:

1. To know security posture
2. To reduce focus area
3. Identify vulnerabilities
4. Draw network map

Footprinting Methodology

- Footprinting through Search Engines
- Footprinting through Advance Google Hacking Techniques
- Footprinting through Social Networking Sites
- Footprinting through Websites
- Footprinting through Email
- Footprinting through Competitive Intelligence
- Footprinting through WHOIS
- Footprinting through DNS
- Footprinting through Network
- Footprinting through Social Engineering



People Search Online Services

There are some online services, popularly used to identify the Phones numbers, Addresses, and People.

Some of these websites include:

www.privateeye.com

www.publicbackgroundchecks.com

www.anywho.com

www.intelius.com

www.4111.com

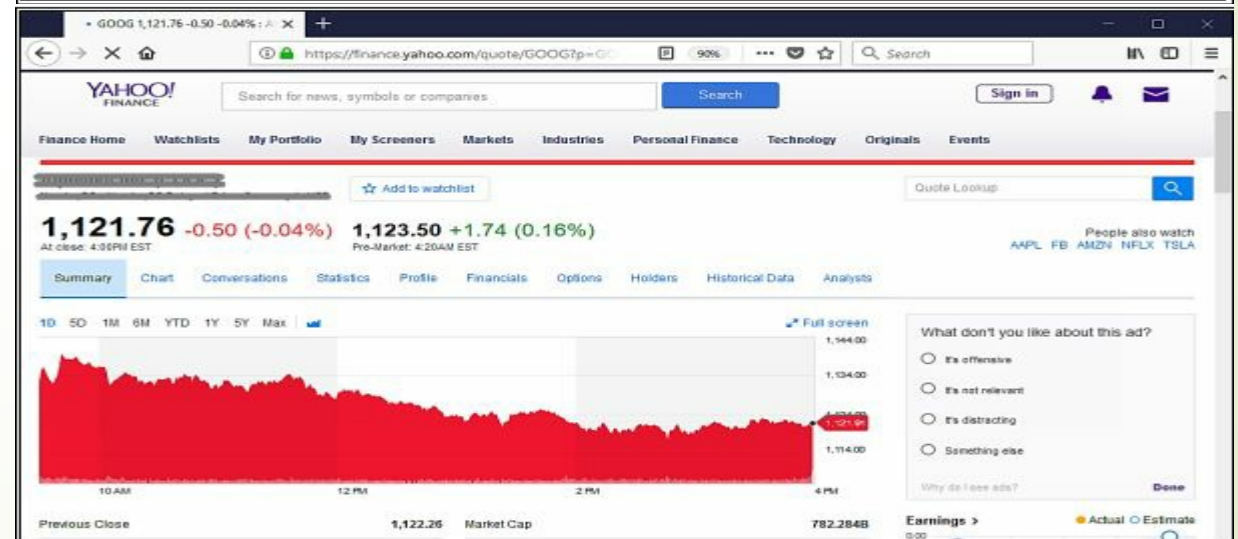
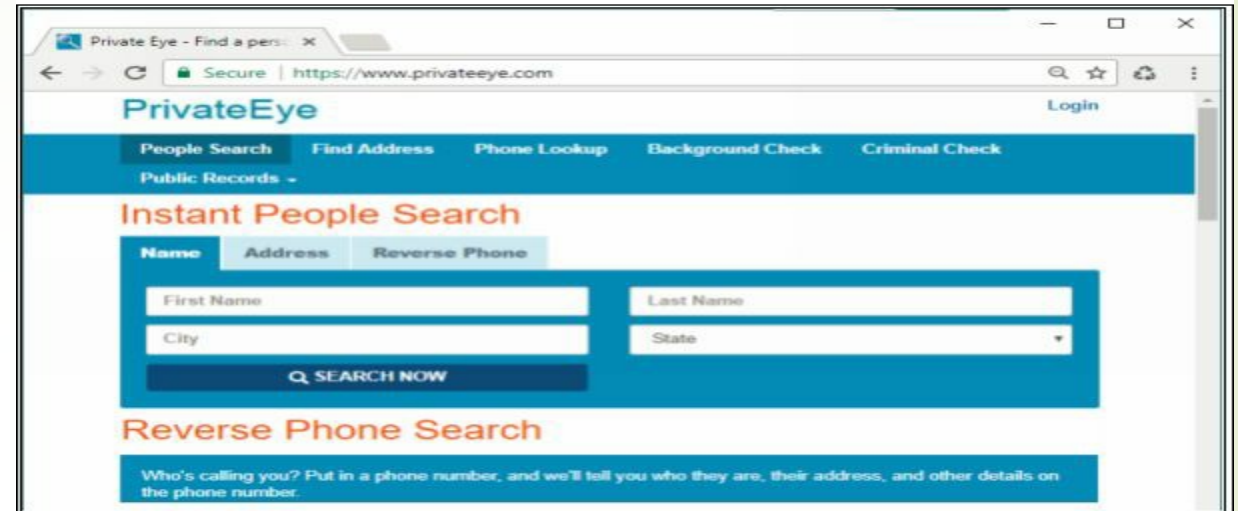
www.peoplefinders.com

Gather Information from Financial Services:

www.google.com/finance

finance.yahoo.com

Footprinting using Advanced Google Hacking Techniques



Website Footprinting

netcraft.com
Shodan.io
censys.io

The screenshot shows the Shodan search interface with the query 'birlasoft'. The results are categorized into several sections:

- TOTAL RESULTS:** 3
- TOP COUNTRIES:** United States (2), India (1)
- TOP SERVICES:** RDP (1), NetBIOS (1), HTTP (1)
- TOP ORGANIZATIONS:** Mahanagar Telephone Nigam (1), Amazon.com (1), Amazon (1)
- TOP PRODUCTS:** Apache httpd (1)

A detailed view of a result for IP 54.82.229.167 is shown, identifying it as an Amazon EC2 instance. A sidebar on the right lists various user roles for the Administrator account, including 'Administrator', 'advhealth', 'birlasoft', 'fnri', 'spirent', 'stihidev', 'stihirun', and 'tdbank'.

The top screenshot shows the Censys search results for 'IPv4 Hosts'. It lists several IP addresses with their associated Autonomous Systems (ASes) and protocols:

- 123.209.91.215:** ASN-TELSTRA Telstra Corporation Ltd (1221), Sydney, New South Wales, Australia. Protocols: 22/ssh.
- 34.89.215.167 (167.215.89.34.bc.googleusercontent.com.):** GOOGLE (15169), United States. Protocols: 22/ssh.
- 54.229.234.118 (ec2-54-229-234-118.eu-west-1.compute.amazonaws.com.):** AMAZON-02 (16509), Dublin, Leinster, Ireland. Protocols: 22/ssh.
- 202.181.102.16 (www1002uo.sakura.ne.jp.):** SAKURA-B SAKURA Internet Inc. (9370), Japan. Protocols: 22/ssh.

The bottom screenshot shows the Netcraft website footprinting results for 'https://birlasoft.com'. It provides detailed information about the site's infrastructure:

- Site:** https://birlasoft.com - Domain registrar: unknown
- Netblock Owner:** Amazon Data Services NoVa - Nameserver organisation: unknown
- Domain:** birlasoft.com - Organisation: unknown
- Nameserver:** auth111.ns.uu.net - Hosting company: unknown
- IP address:** 54.144.67.187 (VirusTotal -) - Top Level Domain: Commercial entities (.com)
- DNS admin:** hostmaster@UU.NET - DNS Security Extensions: unknown
- IPv6 address:** Not Present - Hosting country: US
- Reverse DNS:** ec2-54-144-67-187.compute-1.amazonaws.com

DNS Footprinting

There are a lot of online tools available for DNS lookup information, some of them are listed below:

<https://dnsdumpster.com/>

<http://network-tools.com>

<http://www.kloth.net>

<http://www.mydnstools.info>

<http://www.nirsoft.net>

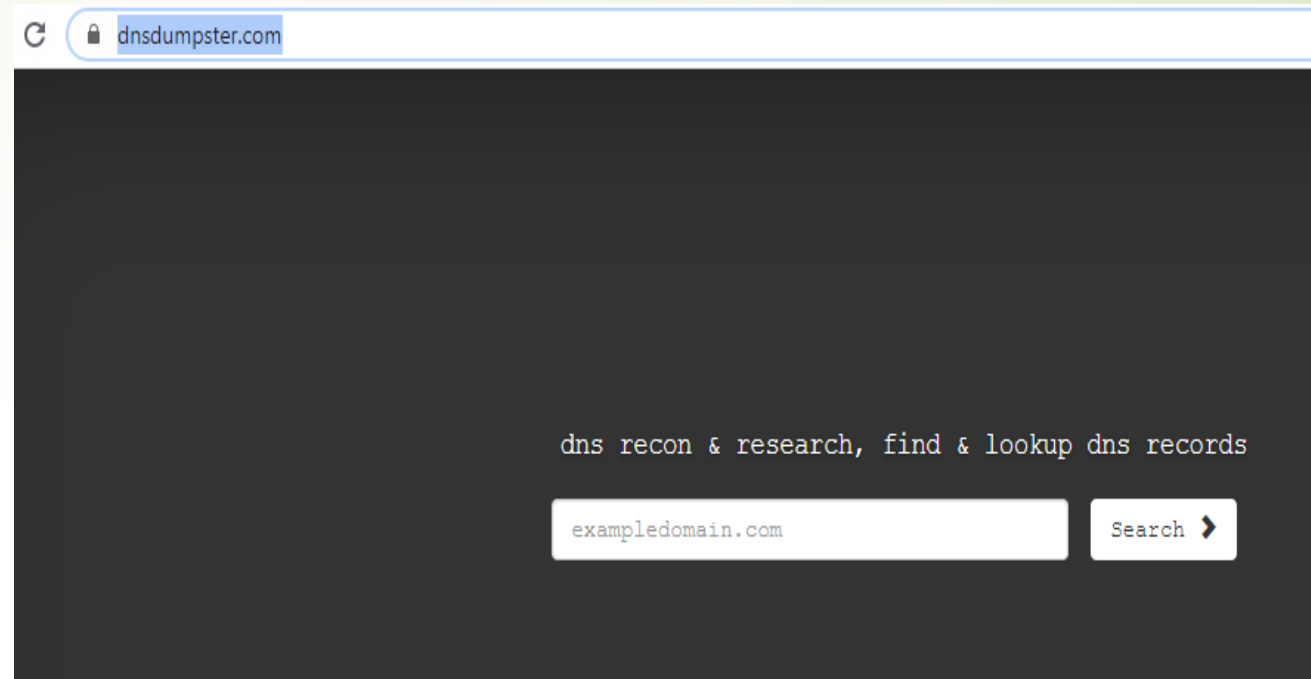
<http://www.dnswatch.info>

<http://www.domaintools.com>

<http://www.dnsqueries.com>

<http://www.ultratools.com>

<http://www.webmaster-toolkit.com>



network-tools.com/#search=dns&search=birlasoft.com&target=_8&form=ntscform&base10toip=false

Tool DNS

Convert Base-10 to IP

birlasoft.com

Go!

Sub Domain Enumeration - Dnsenum

```
root@kali:~# dnsenum --enum google.com
```

```
dnsenum.pl VERSION:1.2.3
```

Host's addresses:

google.com.	62	IN	A	74.125.130.100
google.com.	62	IN	A	74.125.130.101
google.com.	62	IN	A	74.125.130.102
google.com.	62	IN	A	74.125.130.113
google.com.	62	IN	A	74.125.130.138
google.com.	62	IN	A	74.125.130.139

Name Servers:

ns1.google.com.	343227	IN	A	216.239.32.10
ns2.google.com.	343227	IN	A	216.239.34.10
ns3.google.com.	343227	IN	A	216.239.36.10
ns4.google.com.	343227	IN	A	216.239.38.10

Mail (MX) Servers:

aspmx.l.google.com.	17	IN	A	74.125.129.27
alt1.aspmx.l.google.com.	38	IN	A	74.125.142.26
alt3.aspmx.l.google.com.	178	IN	A	173.194.68.27
alt4.aspmx.l.google.com.	163	IN	A	74.125.131.27
alt2.aspmx.l.google.com.	293	IN	A	74.125.137.27

Sub Domain Enumeration - Dmitry

Dmitry -wnspb target.com

```
root@kali:~# dmitry -w facebook.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:31.13.79.35
HostName:facebook.com

Gathered Inic-whois information for facebook.com
-----
Domain Name: FACEBOOK.COM
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: http://www.registrarsafe.com
Updated Date: 2019-10-17T18:52:06Z
Creation Date: 1997-03-29T05:00:00Z
Registry Expiry Date: 2028-03-30T04:00:00Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1-650-308-7004
us: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibit
ed
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibit
```