CSE3501 INFORMATION SECURITY ANALYSIS AND AUDIT

EXERCISE – 10

DATE: 01.10.2020

PENETRATION TESTING

NAME:P.NITYASREE

REGNO: 17MIS1007

1. Footprints and Reconnaissance Tools

Active and passive intelligence:

Passive:

Indistinguishable from ordinary public traffic

Google search and browse company web page

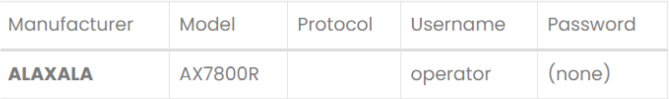
Active:

Network scan,vlnerability scan,ping sweep,

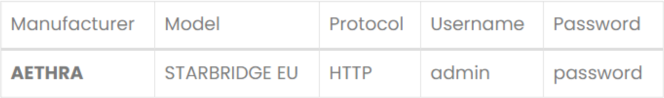
social engineer, spear phishing

Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system.

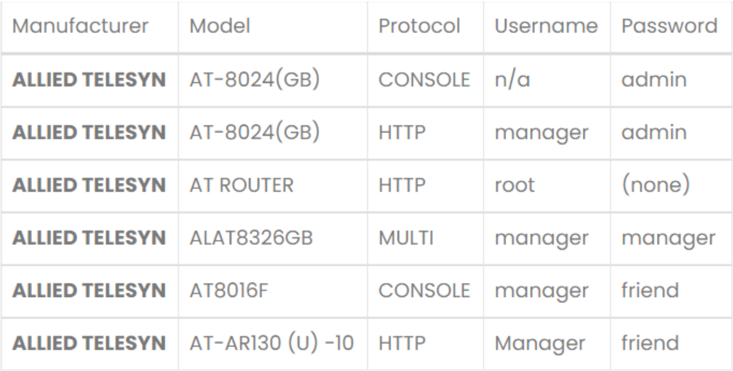
Foot print of manufacturer,model,username,password in routerspasswords.com



Manufacturer	Model	Protocol	Username	Password
ALAXALA	AX7800R		operator	(none)



Manufacturer	Model	Protocol	Username	Password
AETHRA	STARBRIDGE EU	HTTP	admin	password

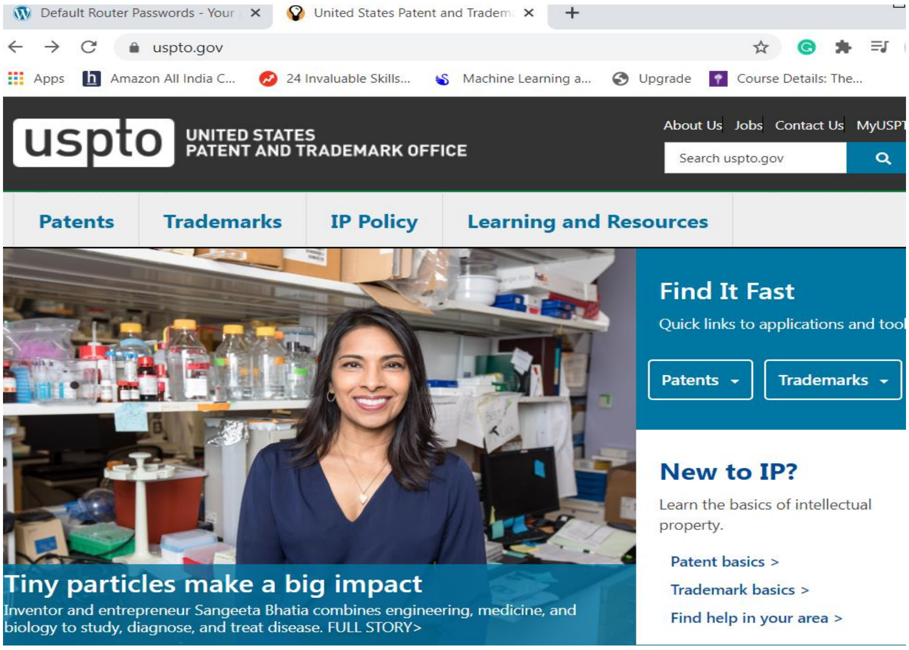


Manufacturer	Model	Protocol	Username	Password
ALLIED TELESYN	AT-8024(GB)	CONSOLE	n/a	admin
ALLIED TELESYN	AT-8024(GB)	HTTP	manager	admin
ALLIED TELESYN	AT ROUTER	HTTP	root	(none)
ALLIED TELESYN	ALAT8326GB	MULTI	manager	manager
ALLIED TELESYN	AT8016F	CONSOLE	manager	friend
ALLIED TELESYN	AT-AR130 (U) -10	HTTP	Manager	friend

2. Information Gathering in Kali Linux

All the information is gathered as public records,corporate fillings such as copyrights,patents and example as **UNITED STATES PATENT AND TRADEMARK OFFICE**

In this page we can find all the latest patents, trademark basics



Find It Fast

Quick links to applications and tool

New to IP?

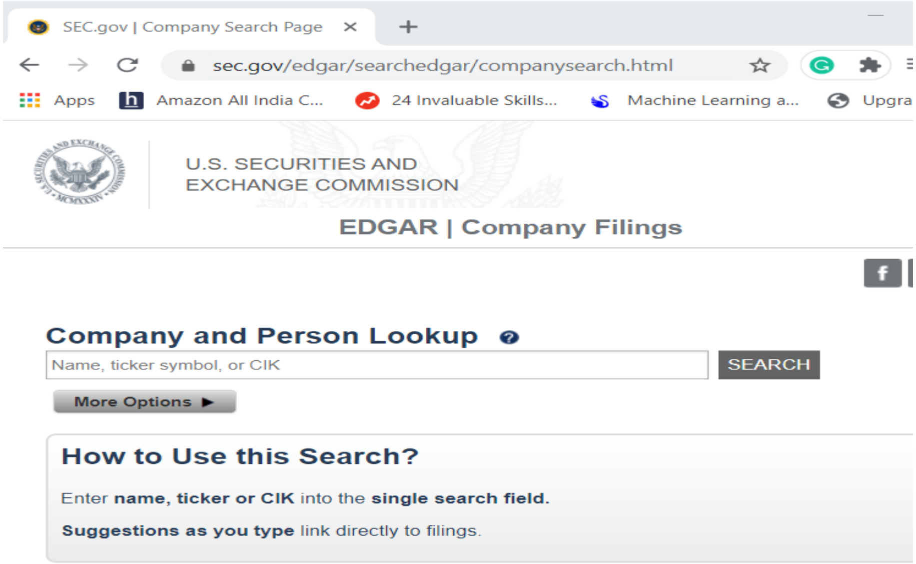
Learn the basics of intellectual property.

Tiny particles make a big impact

Inventor and entrepreneur Sangeeta Bhatia combines engineering, medicine, and biology to study, diagnose, and treat disease. FULL STORY>

The United States Patent and Trademark Office (USPTO) is the federal agency for granting U.S. patents and registering trademarks.

EDGAR


SEC.gov | Company Search Page
sec.gov/edgar/searchedgar/companysearch.html
Apps
Amazon All India C...
24 Invaluable Skills...
Machine Learning a...
Upgra
U.S. SECURITIES AND EXCHANGE COMMISSION
EDGAR | Company Filings
Company and Person Lookup
Name, ticker symbol, or CIK
SEARCH
More Options ▶

How to Use this Search?

Enter **name, ticker or CIK** into the **single search field.**

Suggestions as you type link directly to filings.

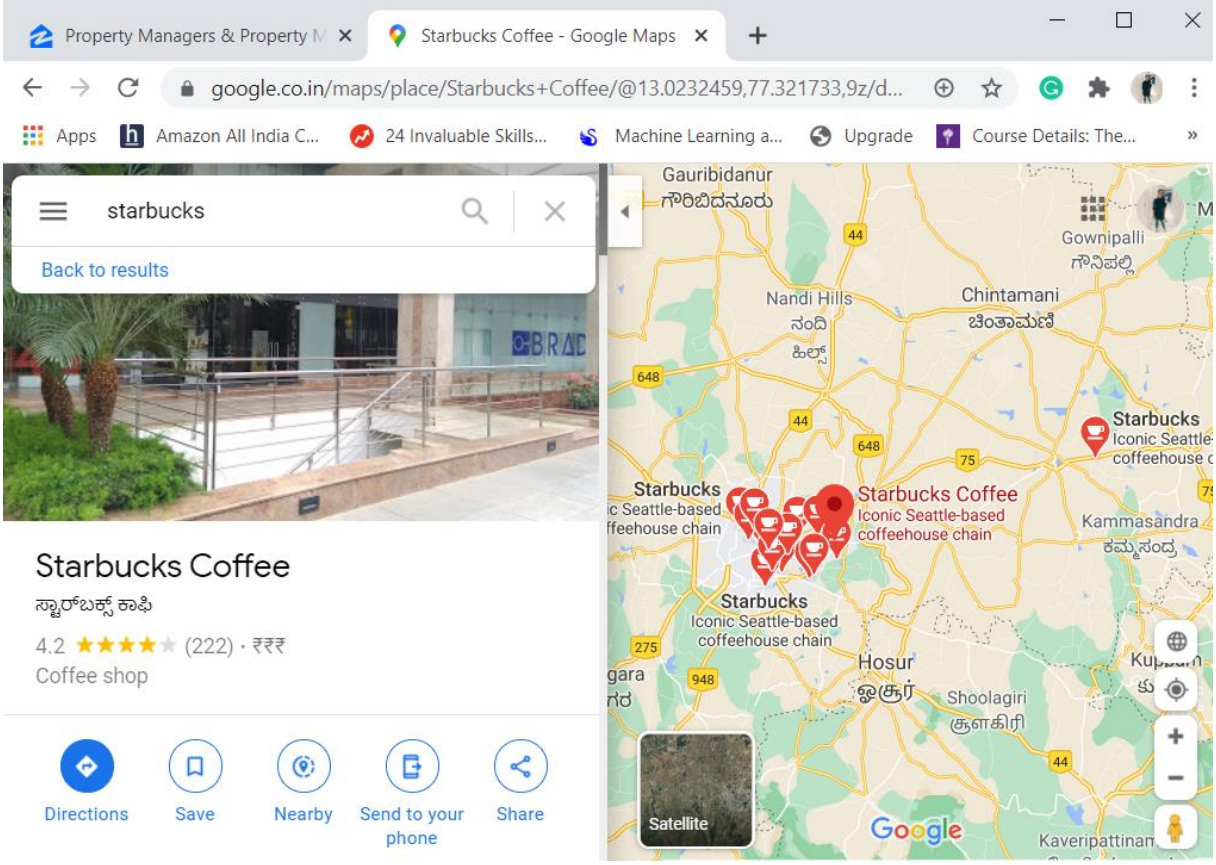
All companies, foreign and domestic, are required to file registration statements, periodic reports, and other forms electronically through EDGAR. Anyone can access and download this information for free.

The quickest way to access EDGAR search tools is to go to Filings & Forms on sec.gov. Besides providing information on corporations, the database also contains information about mutual funds and variable annuities

Google maps – Zillow

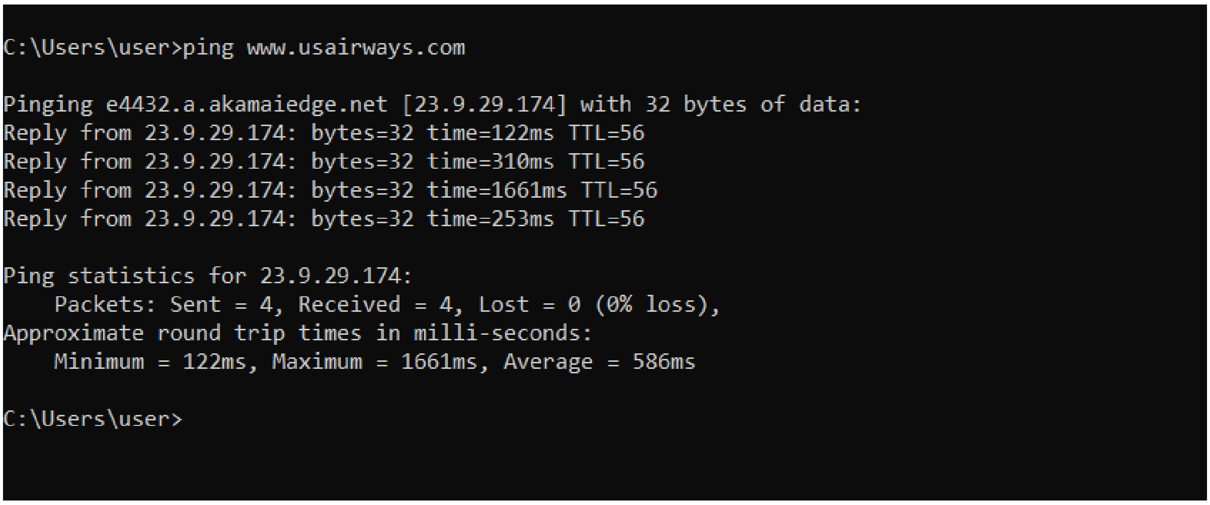
Zillow Group, Inc.

Is an American online real estate database company that was founded in 2006. It helps to find the places for buy,rent or sale and all other information.

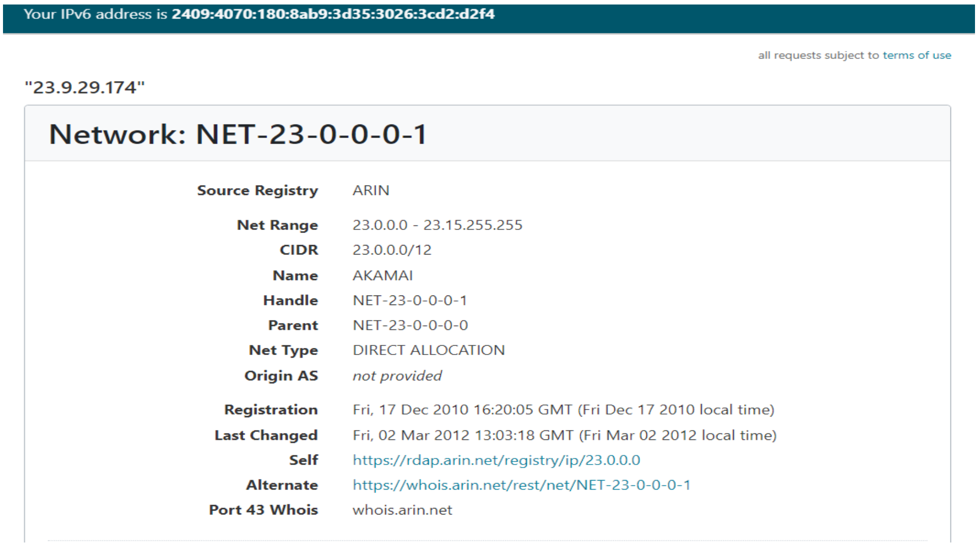


SOCIAL MEDIA:

3. Google Hacking for Penetration Testing



```
C:\Users\user>ping www.usairways.com

Pinging e4432.a.akamaiedge.net [23.9.29.174] with 32 bytes of data:
Reply from 23.9.29.174: bytes=32 time=122ms TTL=56
Reply from 23.9.29.174: bytes=32 time=310ms TTL=56
Reply from 23.9.29.174: bytes=32 time=1661ms TTL=56
Reply from 23.9.29.174: bytes=32 time=253ms TTL=56

Ping statistics for 23.9.29.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 122ms, Maximum = 1661ms, Average = 586ms

C:\Users\user>
```



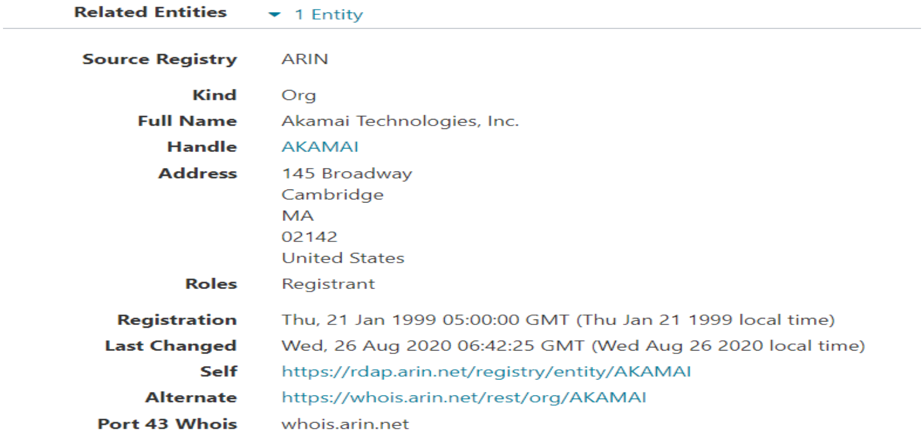
Your IPv6 address is **2409:4070:180:8ab9:3d35:3026:3cd2:d2f4**

all requests subject to terms of use

"23.9.29.174"

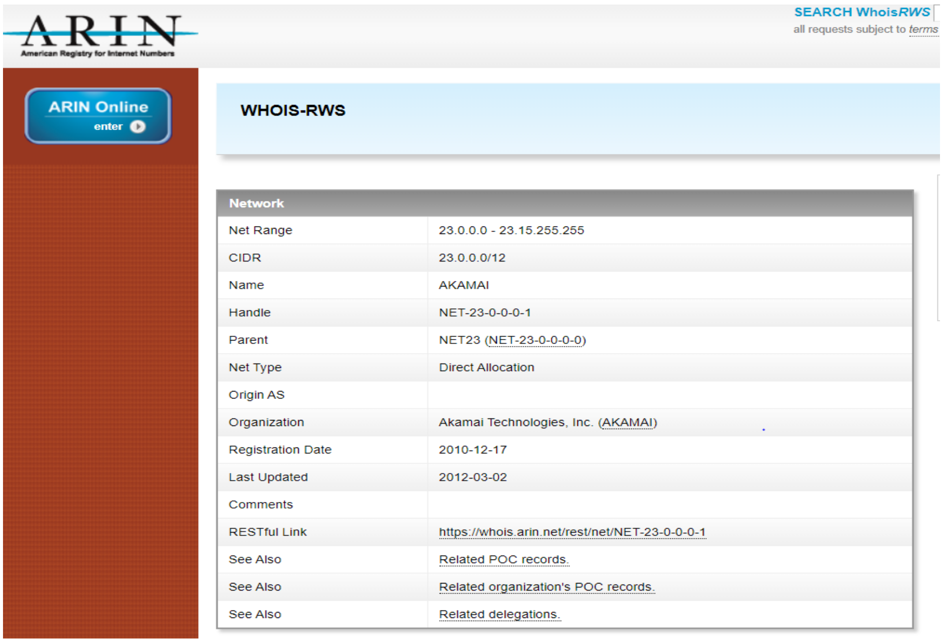
Network: NET-23-0-0-0-1

Source Registry	ARIN
Net Range	23.0.0.0 - 23.15.255.255
CIDR	23.0.0.0/12
Name	AKAMAI
Handle	NET-23-0-0-0-1
Parent	NET-23-0-0-0-0
Net Type	DIRECT ALLOCATION
Origin AS	*not provided*
Registration	Fri, 17 Dec 2010 16:20:05 GMT (Fri Dec 17 2010 local time)
Last Changed	Fri, 02 Mar 2012 13:03:18 GMT (Fri Mar 02 2012 local time)
Self	https://rdap.arin.net/registry/ip/23.0.0.0
Alternate	https://whois.arin.net/rest/net/NET-23-0-0-0-1
Port 43 Whois	whois.arin.net



Related Entities 1 Entity

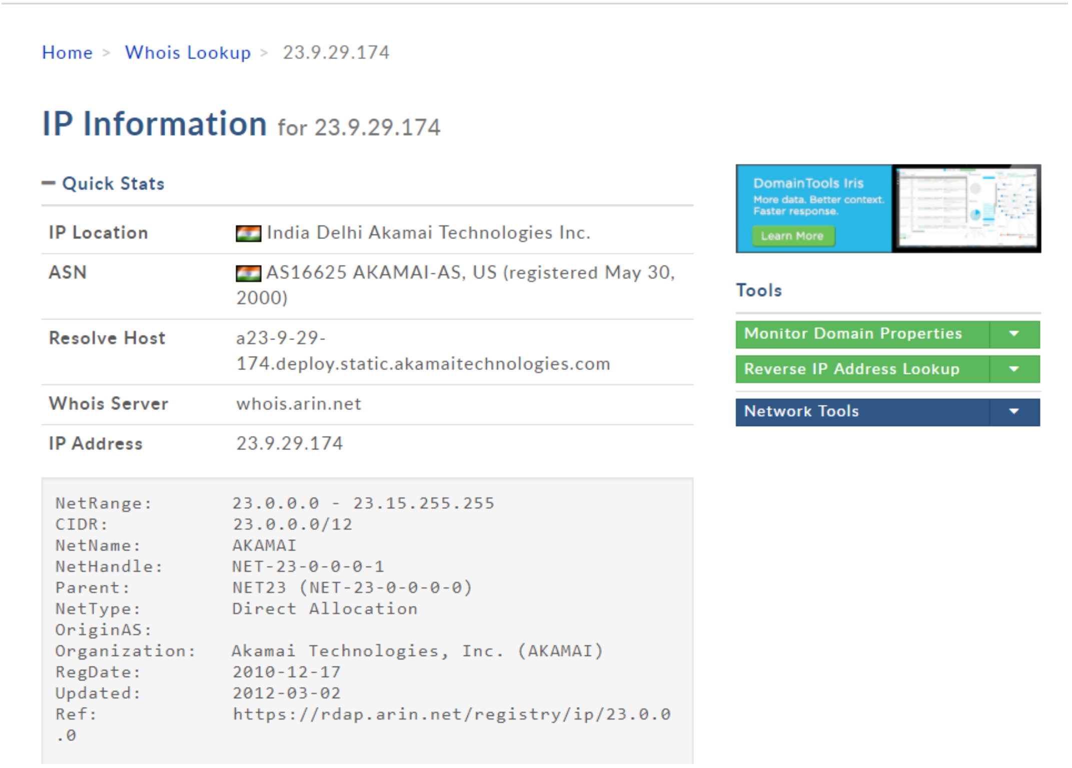
Source Registry	ARIN
Kind	Org
Full Name	Akamai Technologies, Inc.
Handle	AKAMAI
Address	145 Broadway Cambridge MA 02142 United States
Roles	Registrant
Registration	Thu, 21 Jan 1999 05:00:00 GMT (Thu Jan 21 1999 local time)
Last Changed	Wed, 26 Aug 2020 06:42:25 GMT (Wed Aug 26 2020 local time)
Self	https://rdap.arin.net/registry/entity/AKAMAI
Alternate	https://whois.arin.net/rest/org/AKAMAI
Port 43 Whois	whois.arin.net



all requests subject to terms

WHOIS-RWS

Network	
Net Range	23.0.0.0 - 23.15.255.255
CIDR	23.0.0.0/12
Name	AKAMAI
Handle	NET-23-0-0-0-1
Parent	NET23 (NET-23-0-0-0-0)
Net Type	Direct Allocation
Origin AS	
Organization	Akamai Technologies, Inc. (AKAMAI)
Registration Date	2010-12-17
Last Updated	2012-03-02
Comments	
RESTful Link	https://whois.arin.net/rest/net/NET-23-0-0-0-1
See Also	Related POC records.
See Also	Related organization's POC records.
See Also	Related delegations.



IP Information for 23.9.29.174

— Quick Stats

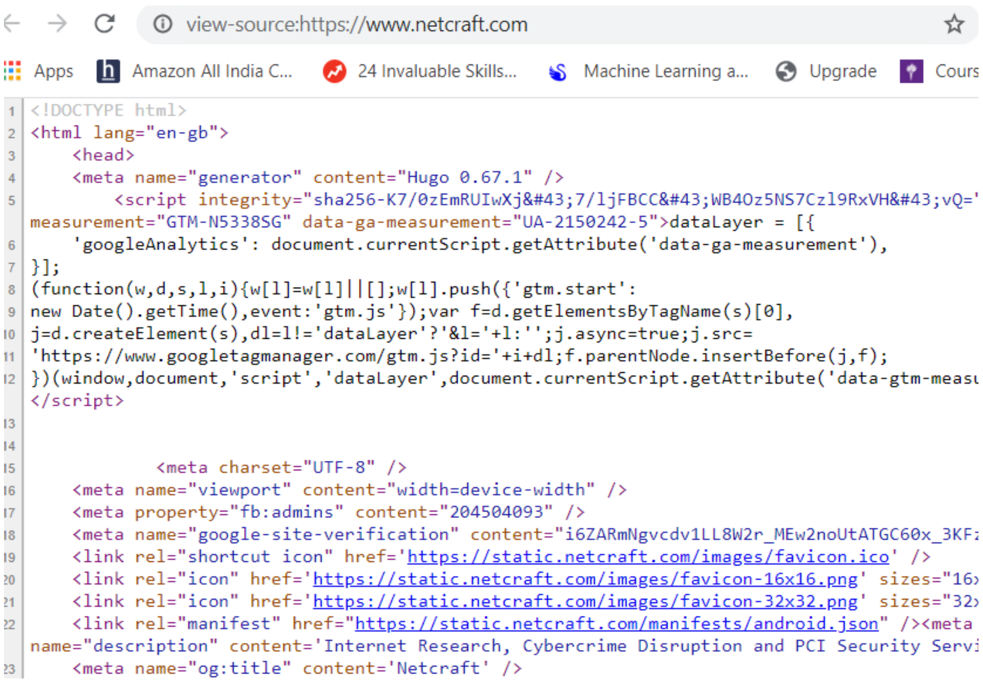
IP Location	India Delhi Akamai Technologies Inc.
ASN	AS16625 AKAMAI-AS, US (registered May 30, 2000)
Resolve Host	a23-9-29-174.deploy.static.akamaitechnologies.com
Whois Server	whois.arin.net
IP Address	23.9.29.174

```
NetRange:       23.0.0.0 - 23.15.255.255
CIDR:           23.0.0.0/12
NetName:        AKAMAI
NetHandle:      NET-23-0-0-0-1
Parent:         NET23 (NET-23-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Akamai Technologies, Inc. (AKAMAI)
RegDate:        2010-12-17
Updated:        2012-03-02
Ref:            https://rdap.arin.net/registry/ip/23.0.0
.0
```

DomainTools Iris
More data. Better context.
Faster response.
Learn More
Tools
Monitor Domain Properties
Reverse IP Address Lookup
Network Tools

Passive recon resources:

Netcraft:



```
<!DOCTYPE html>
<html lang="en-gb">
    <head>
    <meta name="generator" content="Hugo 0.67.1" />
        <script integrity="sha256-K7/0zEmRUIwXj&#43;7/1jFBCC&#43;WB4Oz5NS7Cz19RxVH&#43;vQ='
measurement="GTM-N5338SG" data-ga-measurement="UA-2150242-5">dataLayer = [{
    'googleAnalytics': document.currentScript.getAttribute('data-ga-measurement'),
}];
(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=
'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
})(window,document,'script','dataLayer',document.currentScript.getAttribute('data-gtm-measu
</script>


            <meta charset="UTF-8" />
    <meta name="viewport" content="width=device-width" />
    <meta property="fb:admins" content="204504093" />
    <meta name="google-site-verification" content="i6ZARmNgvcdv1LL8W2r_MEw2noUtATGC60x_3KF:
    <link rel="shortcut icon" href='https://static.netcraft.com/images/favicon.ico' />
    <link rel="icon" href='https://static.netcraft.com/images/favicon-16x16.png' sizes="16
    <link rel="icon" href='https://static.netcraft.com/images/favicon-32x32.png' sizes="32
    <link rel="manifest" href="https://static.netcraft.com/manifests/android.json" /><meta
name="description" content='Internet Research, Cybercrime Disruption and PCI Security Servi
    <meta name="og:title" content='Netcraft' />
```

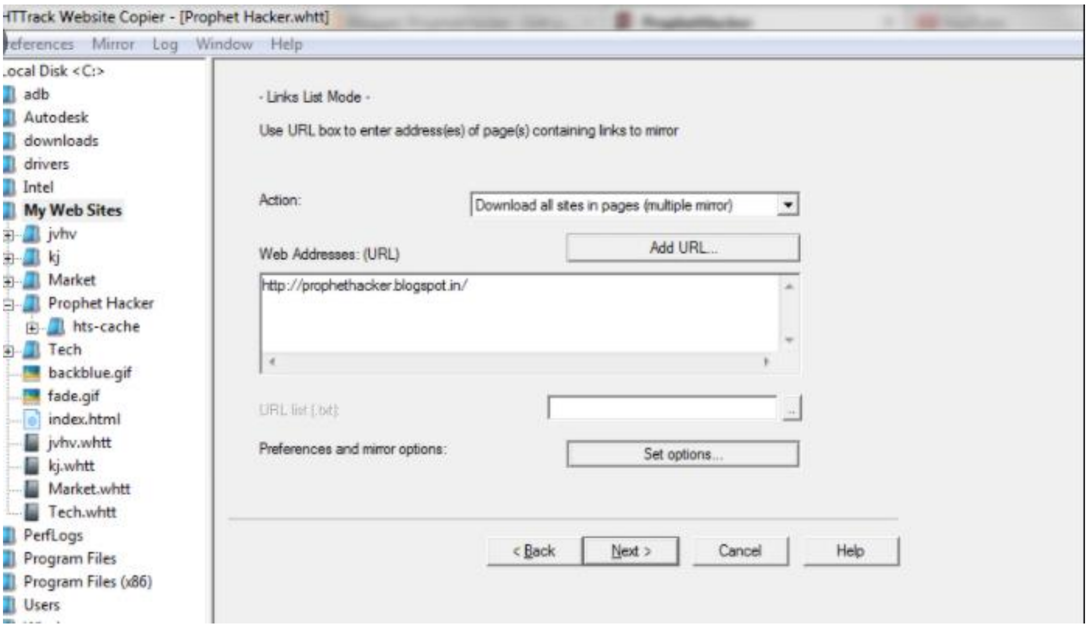
Document grinding, jobs such as search sites, web page source:

Using Sam Spade Footprinting. A security problem is to allow DNS zone transfers from unknown/untrusted Internet users.

The IP block of the target organization, you use pinger to see what hosts are active. Footprinting (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. Sam Spade; TCR trade route; Google searching; HTTrack website copier; Email tracer pro .

4) DNS Spoofing

htttack website copier:



- Links List Mode -

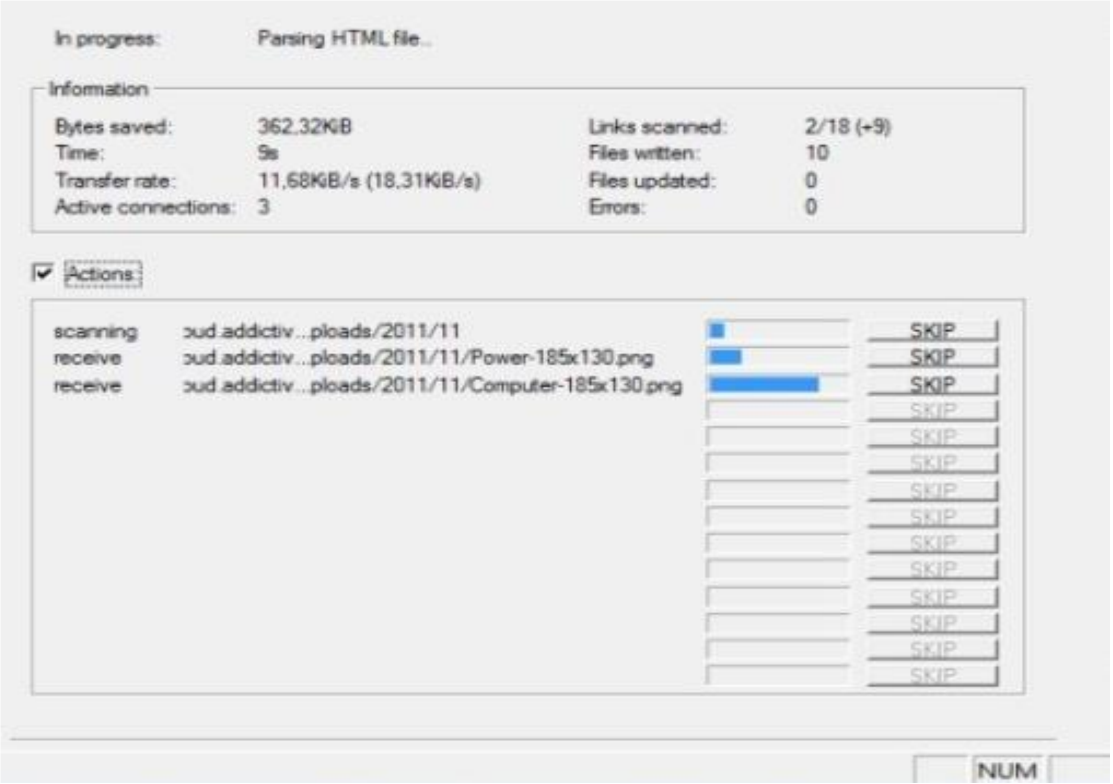
Use URL box to enter address(es) of page(s) containing links to mirror

Action: Download all sites in pages (multiple mirror)

Web Addresses: (URL) http://prophethacker.blogspot.in/

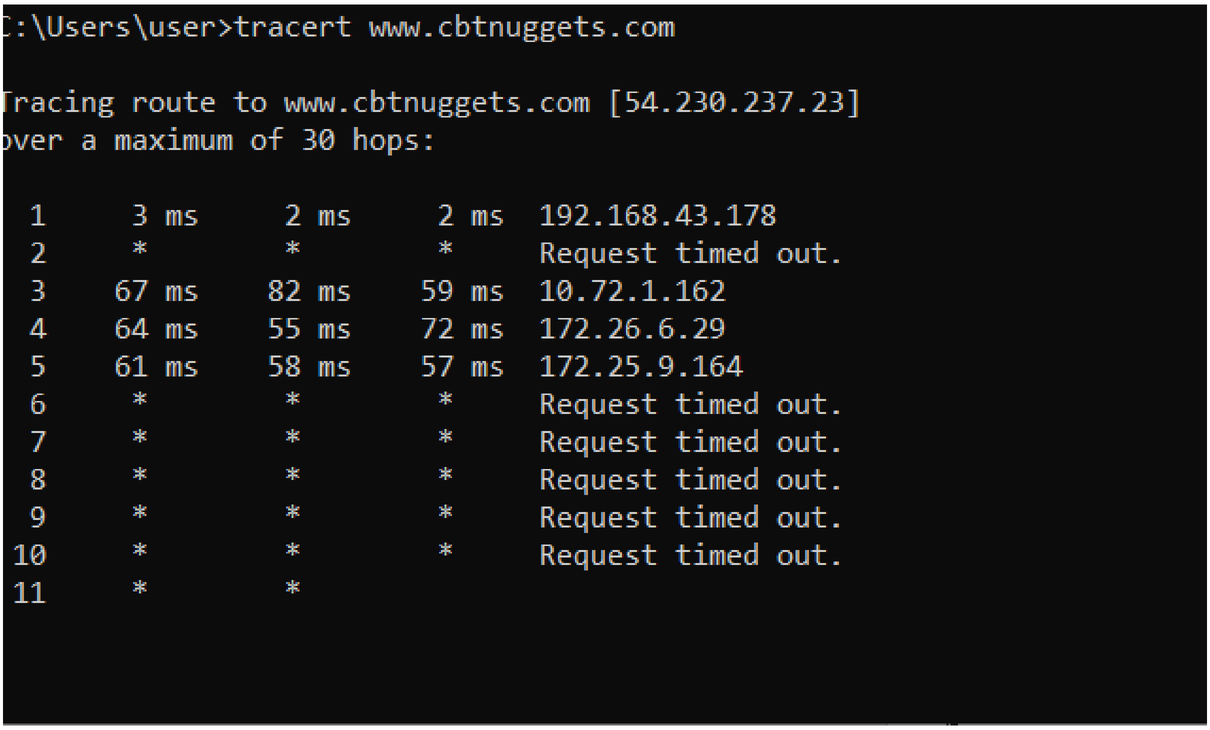
URL list (.txt):

Preferences and mirror options: Set options...



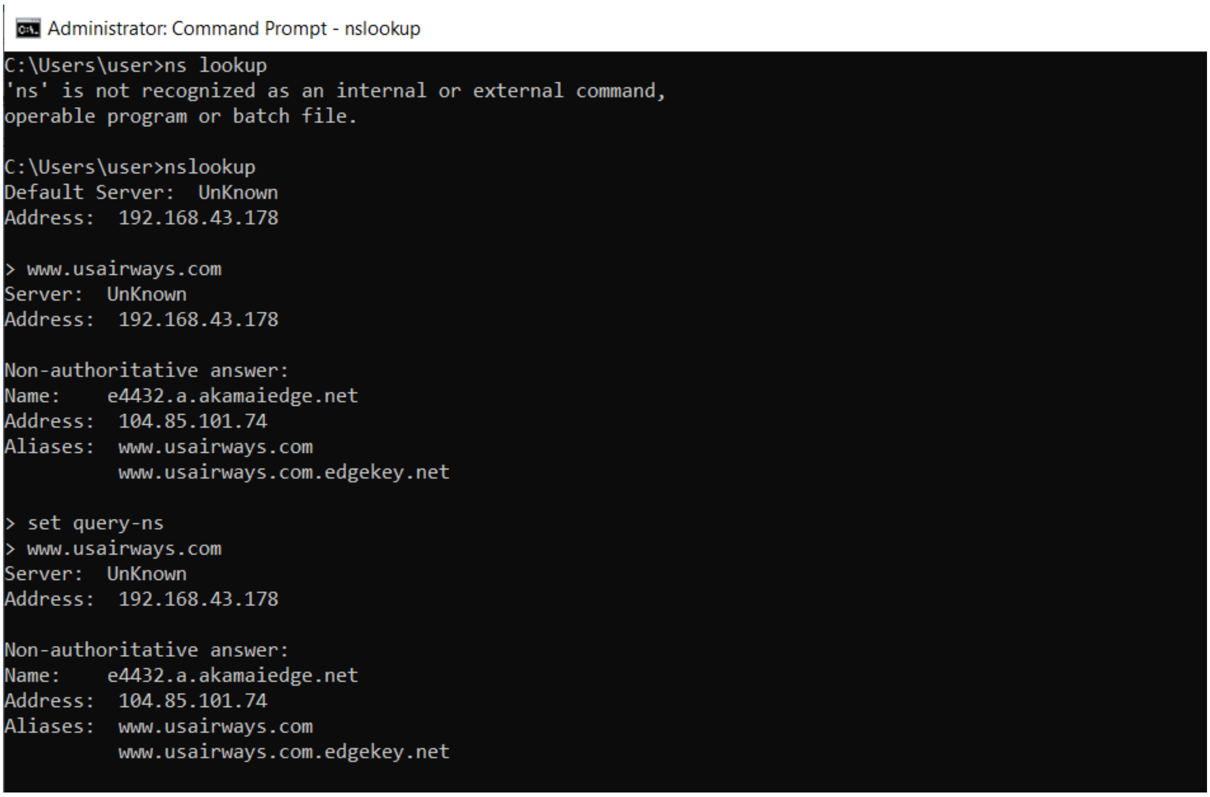
```
In progress:            Parsing HTML file..

Information
Bytes saved:            362,32KiB                       Links scanned:     2/18 (+9)
Time:                   9s                              Files written:     10
Transfer rate:          11,68KiB/s (18,31KiB/s)         Files updated:     0
Active connections:     3                               Errors:            0

☑ Actions:

scanning   oud.addictiv...ploads/2011/11
receive    oud.addictiv...ploads/2011/11/Power-185x130.png
receive    oud.addictiv...ploads/2011/11/Computer-185x130.png
```

Trace route



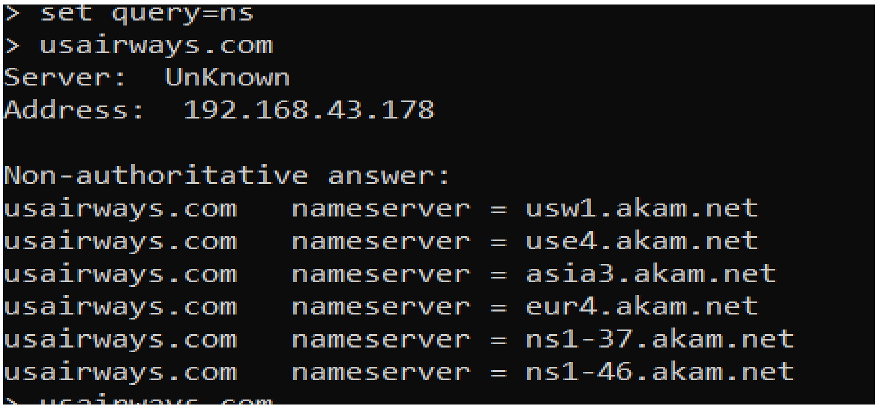
```
C:\Users\user>tracert www.cbtnuggets.com

Tracing route to www.cbtnuggets.com [54.230.237.23]
over a maximum of 30 hops:

  1     3 ms     2 ms     2 ms  192.168.43.178
  2     *        *        *     Request timed out.
  3    67 ms    82 ms    59 ms  10.72.1.162
  4    64 ms    55 ms    72 ms  172.26.6.29
  5    61 ms    58 ms    57 ms  172.25.9.164
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *
```

Dns ns lookup

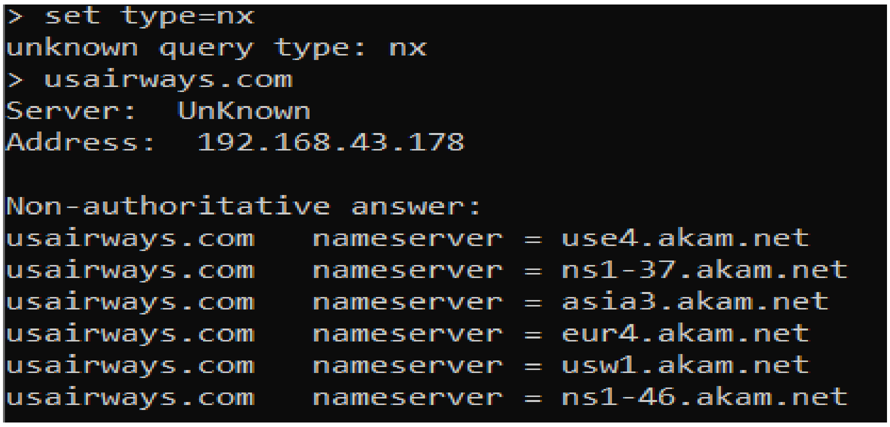


```
C:\Users\user>ns lookup
'ns' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\user>nslookup
Default Server:  UnKnown
Address:  192.168.43.178

> www.usairways.com
Server:  UnKnown
Address:  192.168.43.178

Non-authoritative answer:
Name:    e4432.a.akamaiedge.net
Address:  104.85.101.74
Aliases:  www.usairways.com
          www.usairways.com.edgekey.net

> set query-ns
> www.usairways.com
Server:  UnKnown
Address:  192.168.43.178

Non-authoritative answer:
Name:    e4432.a.akamaiedge.net
Address:  104.85.101.74
Aliases:  www.usairways.com
          www.usairways.com.edgekey.net
```

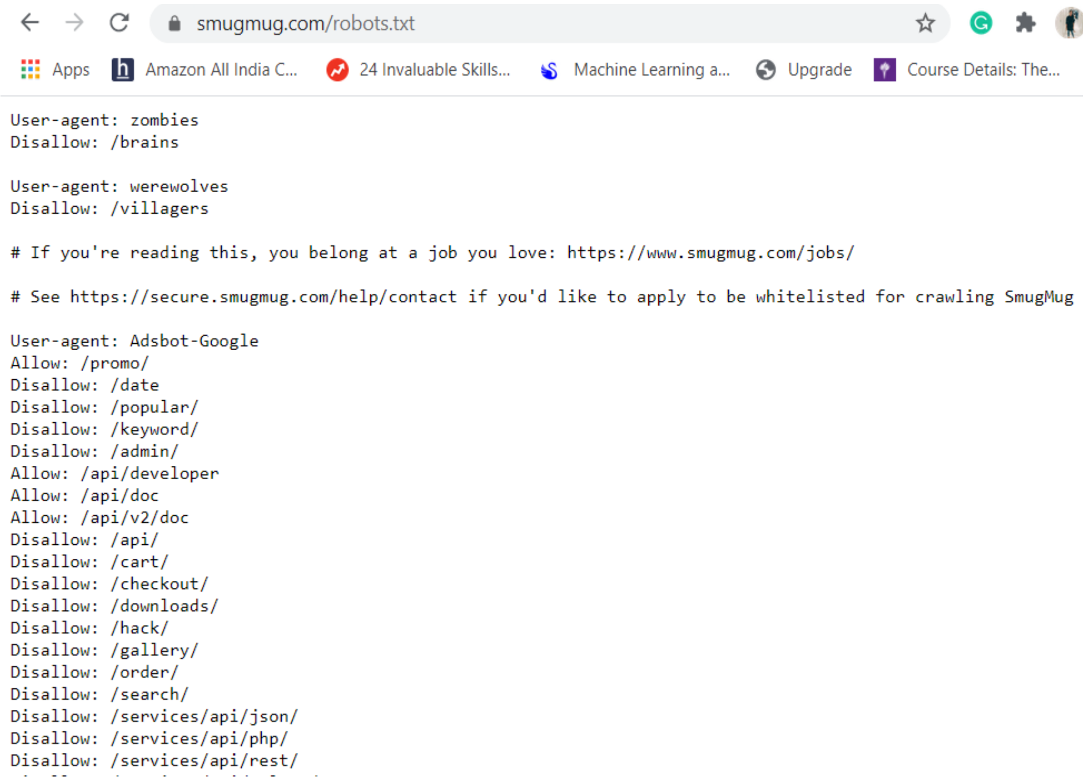
Set type queries:



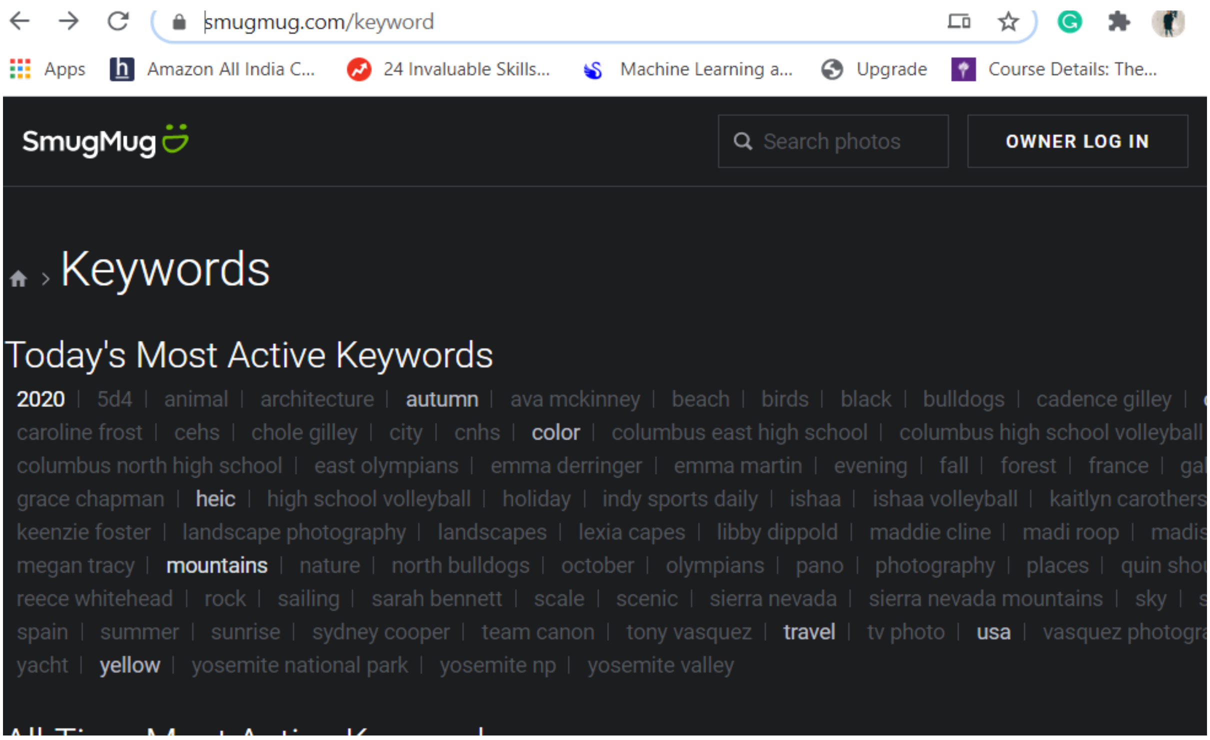
```
> set query=ns
> usairways.com
Server:  UnKnown
Address:  192.168.43.178

Non-authoritative answer:
usairways.com   nameserver = usw1.akam.net
usairways.com   nameserver = use4.akam.net
usairways.com   nameserver = asia3.akam.net
usairways.com   nameserver = eur4.akam.net
usairways.com   nameserver = ns1-37.akam.net
usairways.com   nameserver = ns1-46.akam.net
> usairways.com
```



```
> set type=nx
unknown query type: nx
> usairways.com
Server:  UnKnown
Address:  192.168.43.178

Non-authoritative answer:
usairways.com   nameserver = use4.akam.net
usairways.com   nameserver = ns1-37.akam.net
usairways.com   nameserver = asia3.akam.net
usairways.com   nameserver = eur4.akam.net
usairways.com   nameserver = usw1.akam.net
usairways.com   nameserver = ns1-46.akam.net
```



```
User-agent: zombies
Disallow: /brains

User-agent: werewolves
Disallow: /villagers

# If you're reading this, you belong at a job you love: https://www.smugmug.com/jobs/

# See https://secure.smugmug.com/help/contact if you'd like to apply to be whitelisted for crawling SmugMug

User-agent: Adsbot-Google
Allow: /promo/
Disallow: /date
Disallow: /popular/
Disallow: /keyword/
Disallow: /admin/
Allow: /api/developer
Allow: /api/doc
Allow: /api/v2/doc
Disallow: /api/
Disallow: /cart/
Disallow: /checkout/
Disallow: /downloads/
Disallow: /hack/
Disallow: /gallery/
Disallow: /order/
Disallow: /search/
Disallow: /services/api/json/
Disallow: /services/api/php/
Disallow: /services/api/rest/
```



Keywords

Today's Most Active Keywords

2020 | 5d4 | animal | architecture | autumn | ava mckinney | beach | birds | black | bulldogs | cadence gilley | c
caroline frost | cehs | chole gilley | city | cnhs | color | columbus east high school | columbus high school volleyball
columbus north high school | east olympians | emma derringer | emma martin | evening | fall | forest | france | ga
grace chapman | heic | high school volleyball | holiday | indy sports daily | ishaa | ishaa volleyball | kaitlyn carothers
keenzie foster | landscape photography | landscapes | lexia capes | libby dippold | maddie cline | madi roop | madis
megan tracy | mountains | nature | north bulldogs | october | olympians | pano | photography | places | quin sho
reece whitehead | rock | sailing | sarah bennett | scale | scenic | sierra nevada | sierra nevada mountains | sky | s
spain | summer | sunrise | sydney cooper | team canon | tony vasquez | travel | tv photo | usa | vasquez photogr
yacht | yellow | yosemite national park | yosemite np | yosemite valley

END