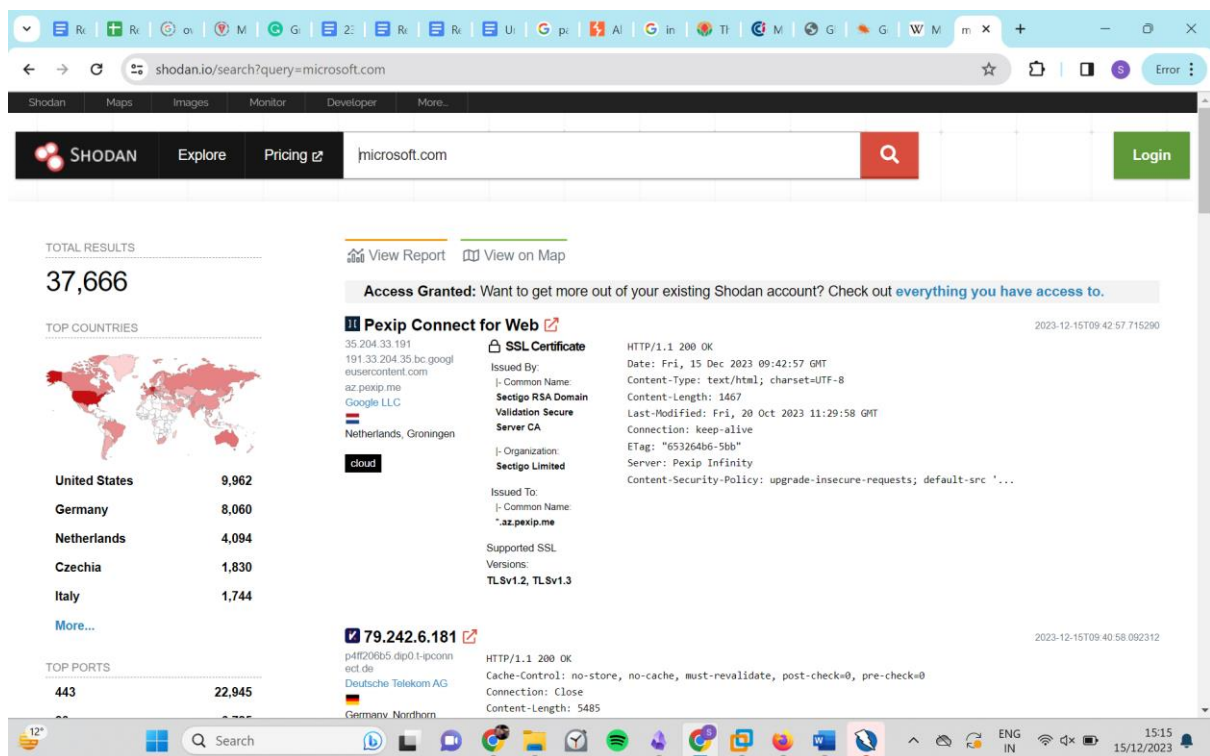


Shaheed Sukhdev College of Business Studies  
University of Delhi  
Post Graduate Diploma in Cyber Security and Law  
Sakshi Garg • Roll no-23726 • Semester-1

## Foot printing

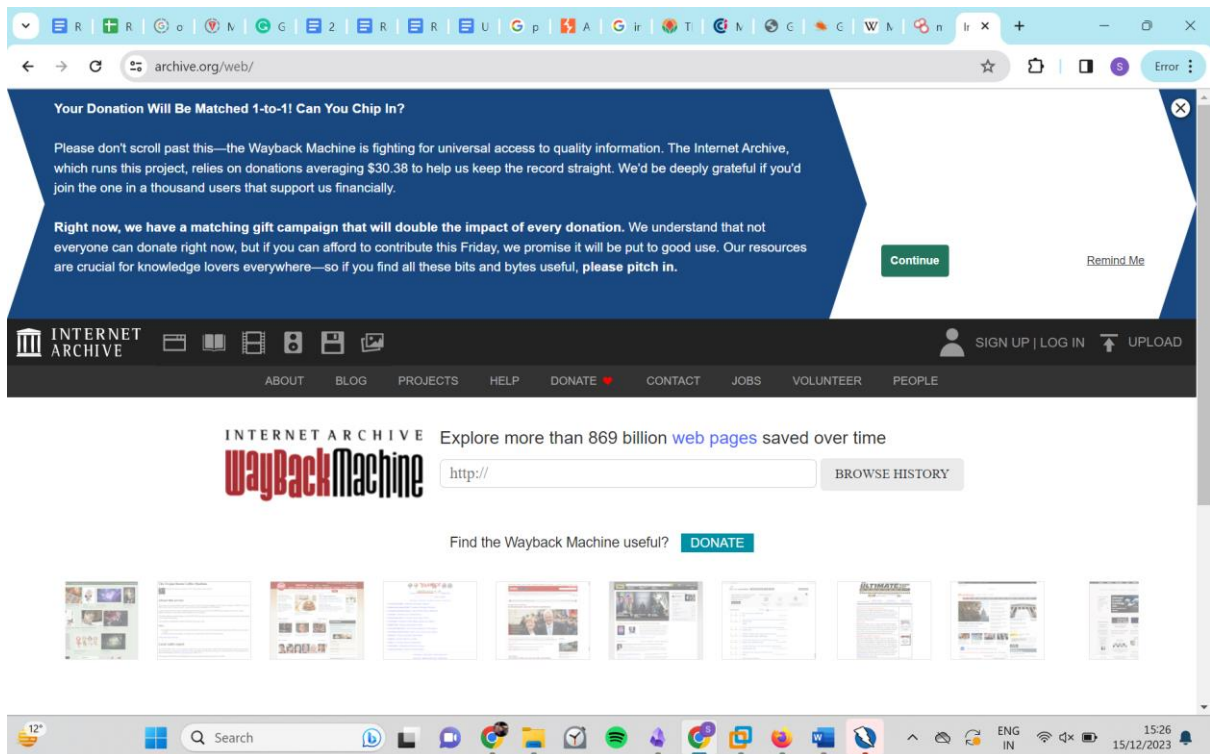
### Shodan Search Engine:

It is a search engine that led user to search for various types of servers connected to the internet using variety of filters. Some have also described it as a search engine of service, banners.

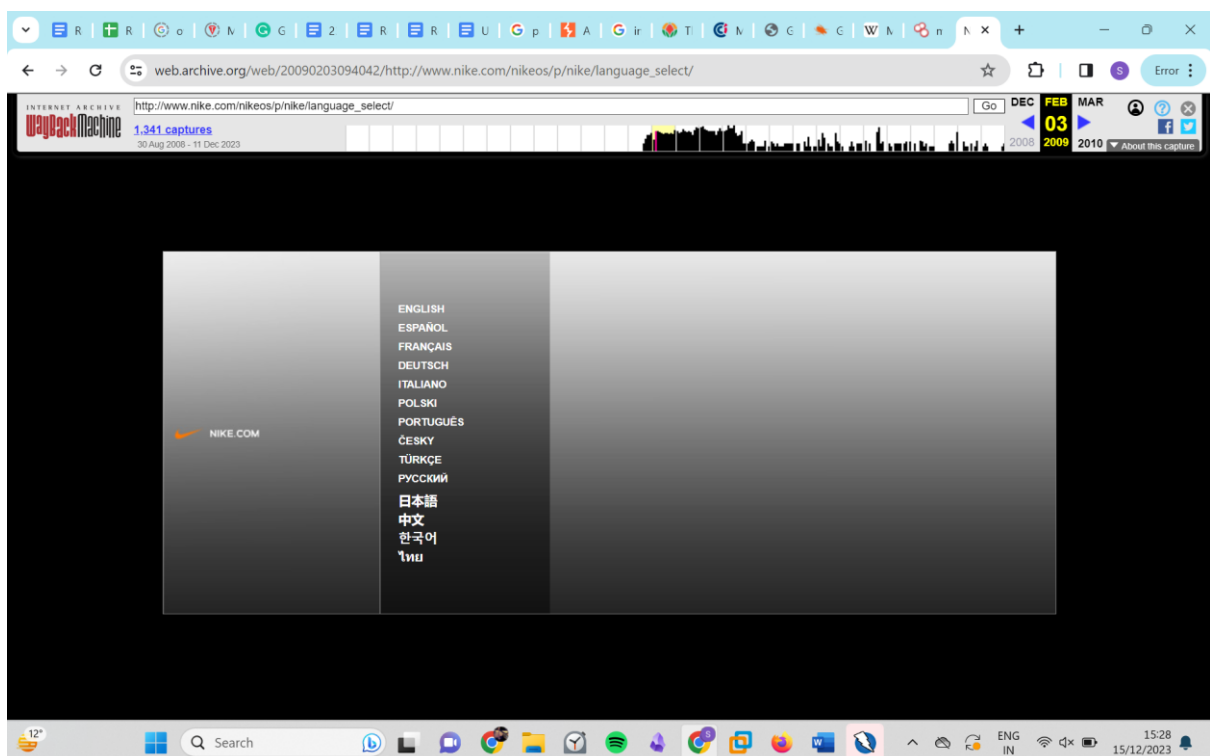


### Way back machine:

It allows the user to go back in time to see how website used to look once

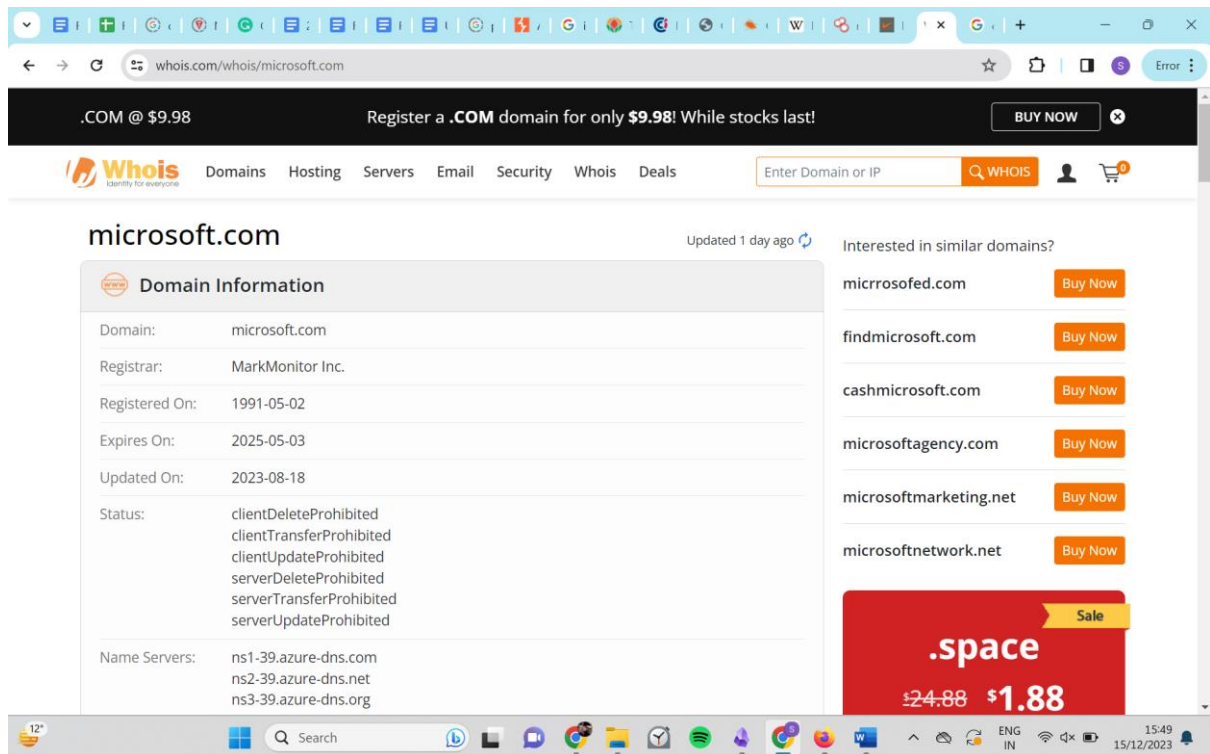
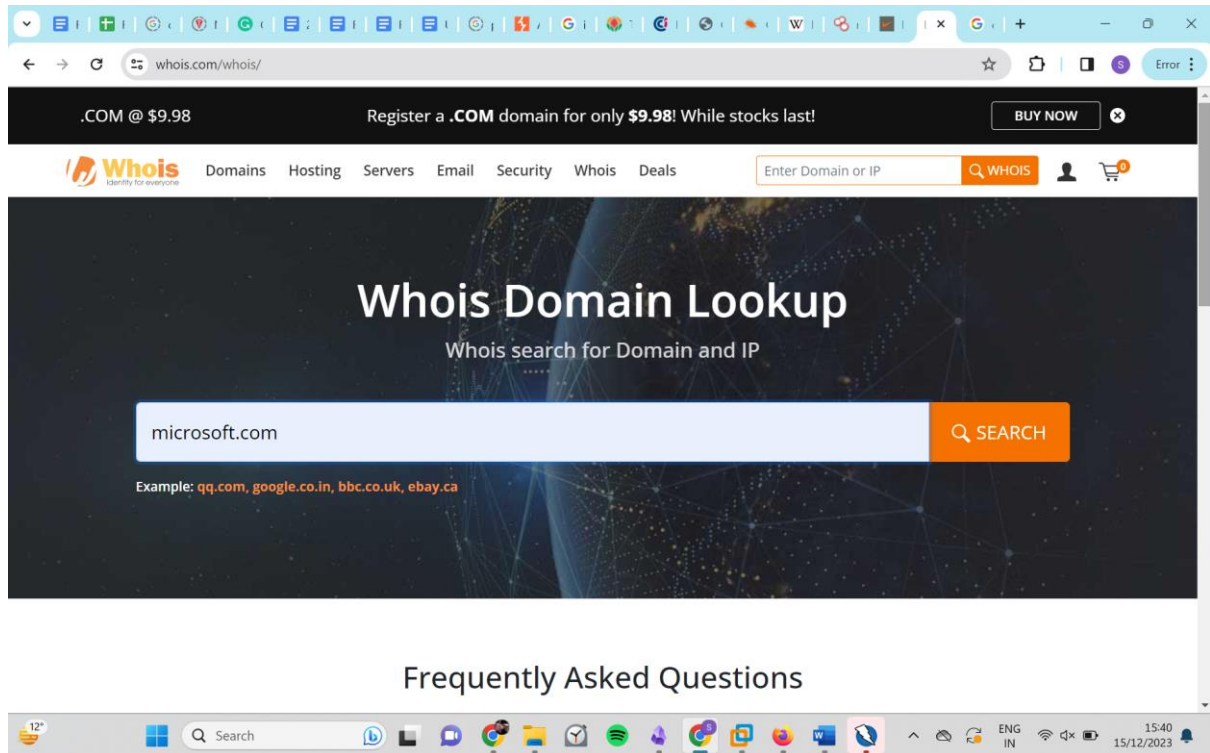


## Example – Nike.com



## Whois Record:

WHOIS is a query and response protocol that is used for querying databases that store an internet resource's registered users or assignees. These resources include domain names, IP address blocks and autonomous systems, but it is also used for a wider range of other information.



whois.com/whois/microsoft.com

.COM @ \$9.98 Register a .COM domain for only \$9.98! While stocks last! BUY NOW

Whois Domains Hosting Servers Email Security Whois Deals Enter Domain or IP WHOIS

### RAW WHOIS Data

```
Domain Name: microsoft.com
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2023-08-18T16:15:54+0000
Creation Date: 1991-05-02T04:00:00+0000
Registrar Registration Expiration Date: 2025-05-03T00:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Microsoft Corporation
Registrant Street: One Microsoft Way,
Registrant City: Redmond
Registrant State/Province: WA
Registrant Postal Code: 98052
```

12° Search ENG IN 15:51 15/12/2023

whois.com/whois/192.168.32.1

.COM @ \$9.98 Register a .COM domain for only \$9.98! While stocks last! BUY NOW

Whois Domains Hosting Servers Email Security Whois Deals Enter Domain or IP WHOIS

### Whois IP 192.168.32.1

Updated 1 day ago

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.
#

NetRange: 192.168.0.0 - 192.168.255.255
CIDR: 192.168.0.0/16
NetName: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle: NET-192-168-0-0-1
Parent: NET192 (NET-192-0-0-0-0)
NetType: IANA Special Use
OriginAS:
Organization: Internet Assigned Numbers Authority (IANA)
RegDate: 1994-03-15
Updated: 2013-08-30
Comment: These addresses are in use by many millions of independently operated networks, w
```

**.space** Sale

~~\$24.88~~ **\$1.88**

BUY NOW

\*while stocks last

**On Sale!**

**.LIVE**

**.LIVE @ \$4.88** ~~\$32.88~~

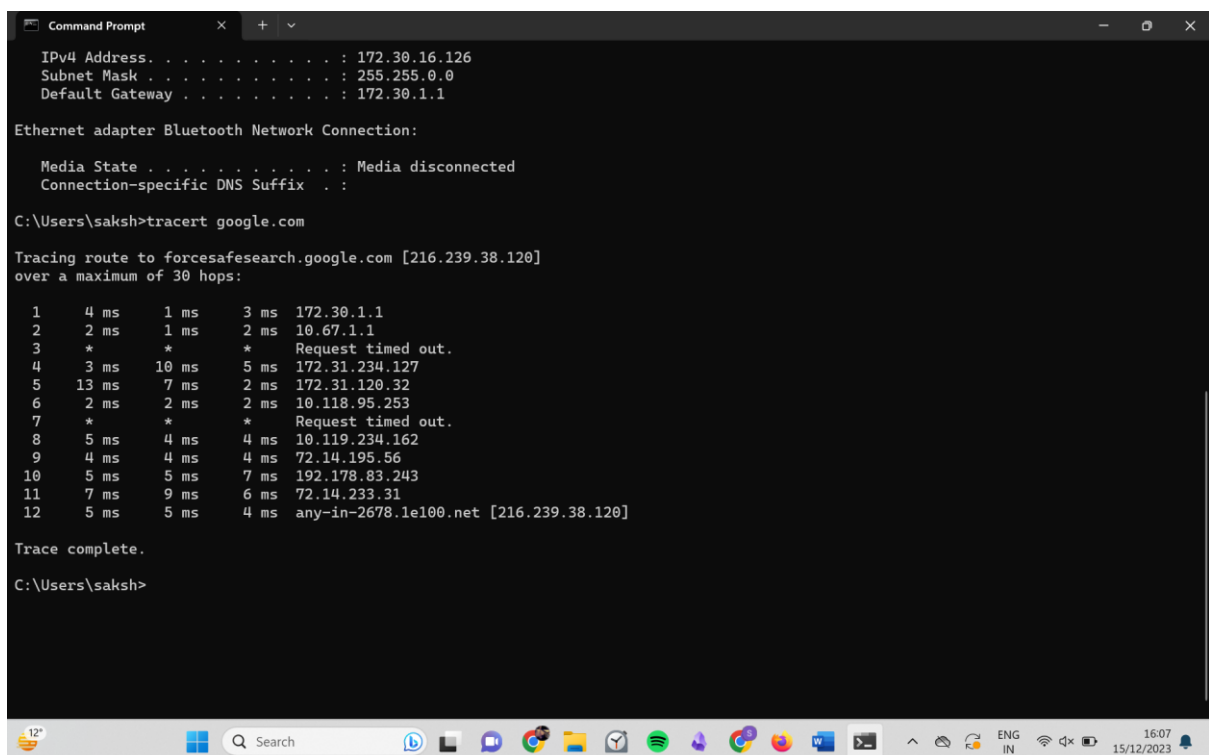
12° Search ENG IN 15:55 15/12/2023

## Tracert:

The window tracert tool determines the root to a destination by sending ICMP Packets to the destination in these packets. Tracert uses varying IP Time-To - Live(TTL) values. The TTL is effectively a hop-counter, where a hop is a location that the packet stops at, to reach destination.

### How to use Tracert

1. Press **Windows key + R** to open the **Run** window.
2. Enter **cmd** and press **Enter** to open a **Command Prompt**.
3. Enter **tracert**, a space, then the IP address or web address for the destination site (for example: tracert www.lexis.com).
4. Press **Enter**.



```
Command Prompt
IPv4 Address. . . . . : 172.30.16.126
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . : 172.30.1.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\saksh>tracert google.com

Tracing route to forcesafesearch.google.com [216.239.38.120]
over a maximum of 30 hops:

  0  4 ms  1 ms  3 ms  172.30.1.1
  1  2 ms  1 ms  2 ms  10.67.1.1
  2  *      *      *      Request timed out.
  3  3 ms  10 ms  5 ms  172.31.234.127
  4  13 ms  7 ms  2 ms  172.31.120.32
  5  2 ms  2 ms  2 ms  10.118.95.253
  6  *      *      *      Request timed out.
  7  5 ms  4 ms  4 ms  10.119.234.162
  8  4 ms  4 ms  4 ms  72.14.195.56
  9  5 ms  5 ms  7 ms  192.178.83.243
 10  7 ms  9 ms  6 ms  72.14.233.31
 11  5 ms  5 ms  4 ms  any-in-2678.1e100.net [216.239.38.120]

Trace complete.

C:\Users\saksh>
```