Assignment 1-2: Connectivity and Discovery Tools

Name: ____

Objective

In this lab, you will learn to use the TCP/IP Packet Internet Groper (Ping), Trace Route (Tracert) and NSLOOKUP commands for testing connectivity in a network. We also look at Whois services. With ping and tracert, you will see name resolution occur using one or more DNS servers.

Scenario

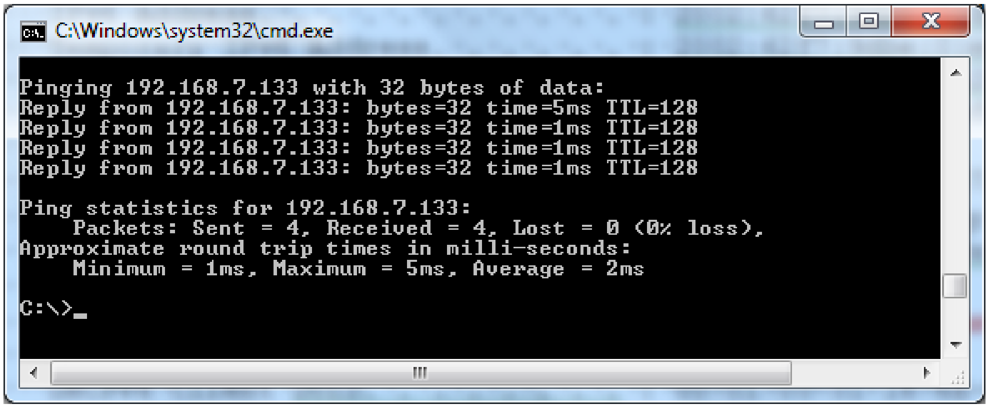
This lab assumes you are using any version of Windows. Mac users should be able to use the Terminal application.

Ideally, this lab will be done in a classroom or other LAN connected to the Internet. You will need the IP addresses that you recorded in Lab 1.

Part 1

Use the **Start** menu and **RUN** to open the **Command Prompt** window.

Type ping followed by the IP address of your computer – you wrote it down on the last exercise. The following figure shows the possible result of pinging your own IP address.



```
Pinging 192.168.7.133 with 32 bytes of data:
Reply from 192.168.7.133: bytes=32 time=5ms TTL=128
Reply from 192.168.7.133: bytes=32 time=1ms TTL=128
Reply from 192.168.7.133: bytes=32 time=1ms TTL=128
Reply from 192.168.7.133: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.7.133:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\>_
```

Ping uses the ICMP “echo reply” feature to test connectivity. Since it reports on four attempts, you have an indication of the reliability of the connection. Look over your results.

Note: Windows’ firewall may prevent the pings from returning – appear to fail.

Try pinging the default gateway’s IP address if one was listed in the last exercise. If you can, it means you have physical connectivity to the router on your network and therefore probably the rest of the world.

If you are in a classroom or working with a second computer on the network, try pinging the IP address of another machine. Note the results. Try others in the LAN.

Try pinging the IP address of the DHCP and/or DNS servers listed in the last exercise. If it works for either server and they are not on your network, what does that tell you? It means your router is functioning as a default gateway to get you out.

Were you successful? ________________

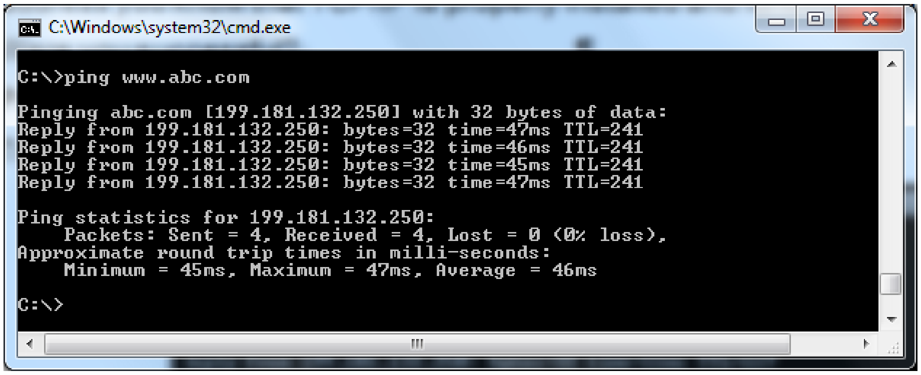
Part 2

Try pinging 127.0.0.1 although it can be any 127 address. The 127 network is reserved for loopback testing – it is pinging your computer. If you can successfully ping the loopback address, you know that TCP/IP is properly installed and functioning on this computer.

Were you successful? ________________

Part 3

Try pinging the **Fully Qualified Domain Name (FQDN)** www.abc.com. Where **www** is the host server, **abc.com** is the domain. Specifically, **ABC** is the domain name and **com** is the **top-level domain (TLD)** – one of the domains at the highest level in the hierarchical Domain Name System of the Internet.



```
C:\>ping www.abc.com

Pinging abc.com [199.181.132.250] with 32 bytes of data:
Reply from 199.181.132.250: bytes=32 time=47ms TTL=241
Reply from 199.181.132.250: bytes=32 time=46ms TTL=241
Reply from 199.181.132.250: bytes=32 time=45ms TTL=241
Reply from 199.181.132.250: bytes=32 time=47ms TTL=241

Ping statistics for 199.181.132.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 45ms, Maximum = 47ms, Average = 46ms

C:\>
```

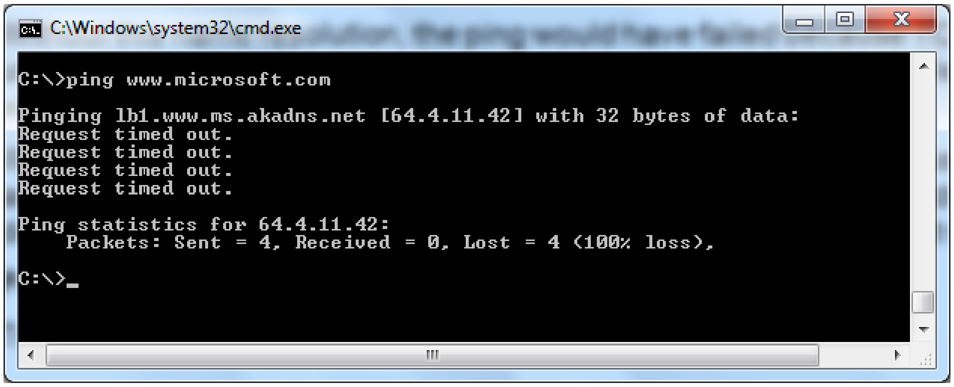
The first line of output shows the domain **abc.com** – followed by the IP address. A (Domain Name Service) DNS server somewhere out in the network resolved the name to an IP address. DNS servers resolve Domain names (not hostnames) to IP addresses.

Without this name resolution, the ping would have failed because TCP/IP (the Internet) only understands valid IP addresses – not names. You would not be able to use your Web browser without this name resolution.

With DNS you can verify connectivity to computers on the Internet using familiar Web addresses (domain names) without having to know the actual IP address. If the nearest DNS server does not know the address, it will ask a server higher in the Internet structure.

Part 4

Try pinging www.microsoft.com. You might get a result like this. What does it mean?



```
C:\>ping www.microsoft.com

Pinging lb1.www.ms.akadns.net [64.4.11.42] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 64.4.11.42:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>_
```

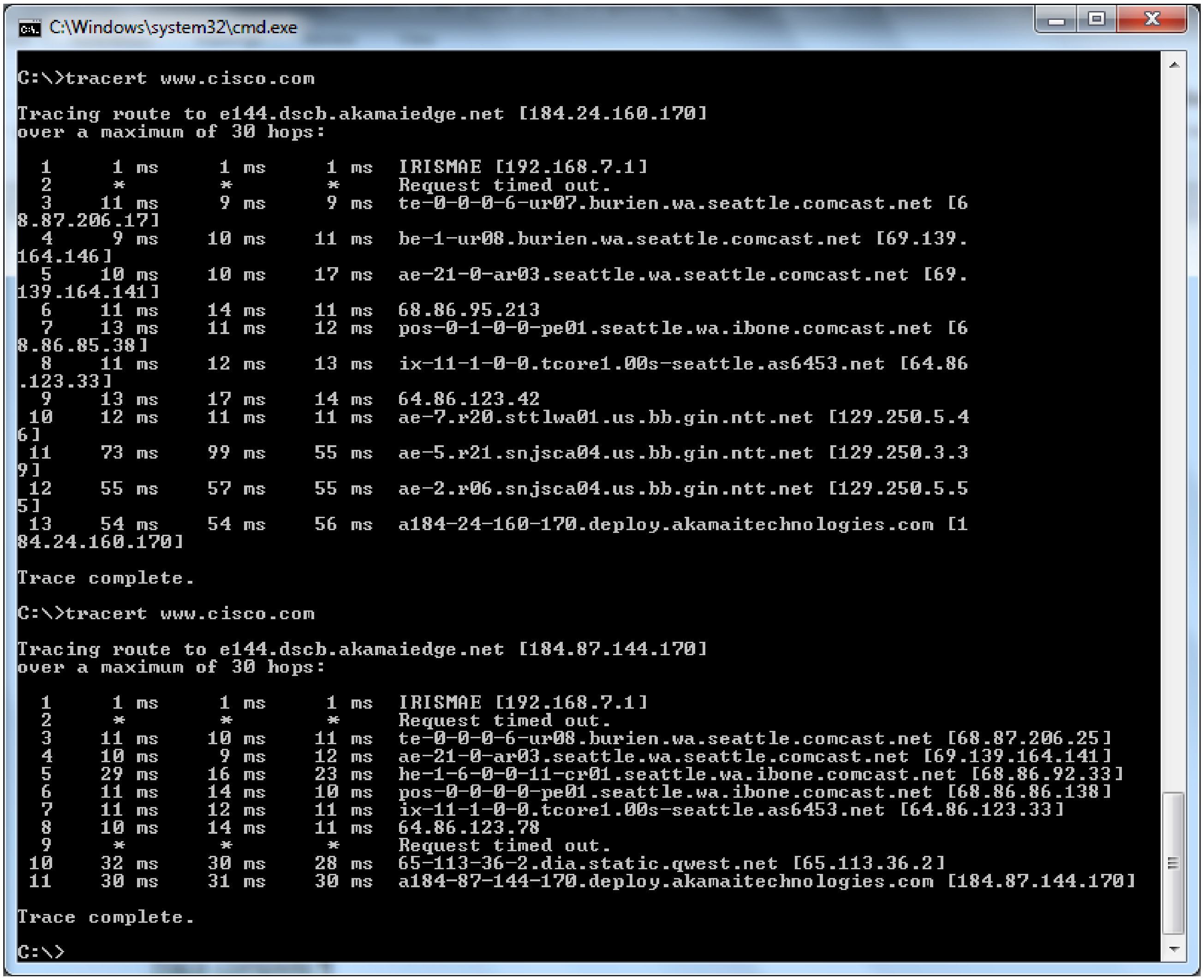
Notice that the DNS server could resolve the name to an IP address, but you get no response. The routers have been configured to ignore ping requests. This is a security measure that many networks implement today – thanks to all the bad guys that used ping to verify addresses.

Try to ping several other domain names including www.uw.edu and ischool.uw.edu that you are aware of and record the results: Notice that the iSchool's host server isn't named **www**.

Example: www.msn.de or IP: 207.46.28.116 Timed out 4 times (MSN in Germany)

Part 5 –TRACERT and Customizing the Command Window

Try typing **tracert www.cisco.com** and press Enter.

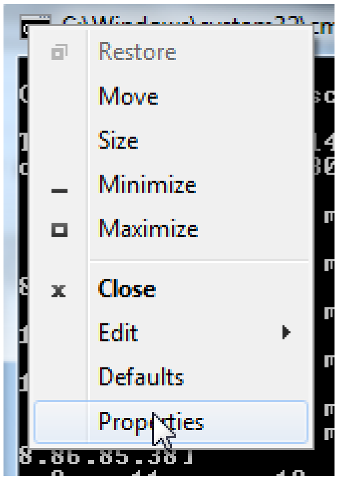


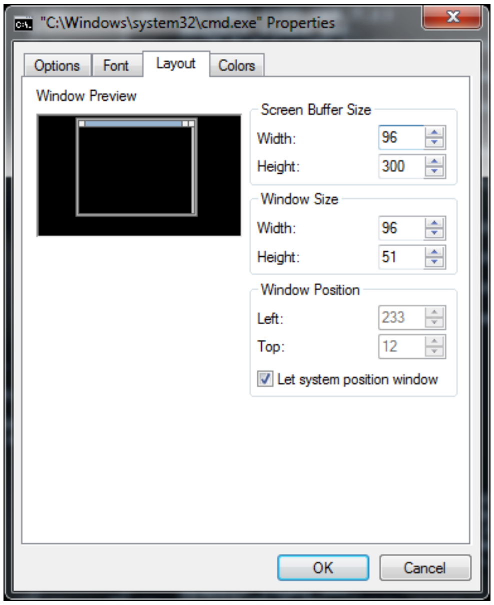
```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [184.24.160.170]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  IRISMAE [192.168.7.1]
  2     *        *        *     Request timed out.
  3    11 ms     9 ms     9 ms  te-0-0-0-6-ur07.burien.wa.seattle.comcast.net [6
8.87.206.17]
  4     9 ms    10 ms    11 ms  be-1-ur08.burien.wa.seattle.comcast.net [69.139.
164.146]
  5    10 ms    10 ms    17 ms  ae-21-0-ar03.seattle.wa.seattle.comcast.net [69.
139.164.141]
  6    11 ms    14 ms    11 ms  68.86.95.213
  7    13 ms    11 ms    12 ms  pos-0-1-0-0-pe01.seattle.wa.ibone.comcast.net [6
8.86.85.38]
  8    11 ms    12 ms    13 ms  ix-11-1-0-0.tcore1.00s-seattle.as6453.net [64.86
.123.33]
  9    13 ms    17 ms    14 ms  64.86.123.42
 10    12 ms    11 ms    11 ms  ae-7.r20.sttlwa01.us.bb.gin.ntt.net [129.250.5.4
6]
 11    73 ms    99 ms    55 ms  ae-5.r21.snjsca04.us.bb.gin.ntt.net [129.250.3.3
9]
 12    55 ms    57 ms    55 ms  ae-2.r06.snjsca04.us.bb.gin.ntt.net [129.250.5.5
5]
 13    54 ms    54 ms    56 ms  a184-24-160-170.deploy.akamaitechnologies.com [1
84.24.160.170]

Trace complete.

C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [184.87.144.170]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  IRISMAE [192.168.7.1]
  2     *        *        *     Request timed out.
  3    11 ms    10 ms    11 ms  te-0-0-0-6-ur08.burien.wa.seattle.comcast.net [68.87.206.25]
  4    10 ms     9 ms    12 ms  ae-21-0-ar03.seattle.wa.seattle.comcast.net [69.139.164.141]
  5    29 ms    16 ms    23 ms  he-1-6-0-0-11-cr01.seattle.wa.ibone.comcast.net [68.86.92.33]
  6    11 ms    14 ms    10 ms  pos-0-0-0-0-pe01.seattle.wa.ibone.comcast.net [68.86.86.138]
  7    11 ms    12 ms    11 ms  ix-11-1-0-0.tcore1.00s-seattle.as6453.net [64.86.123.33]
  8    10 ms    14 ms    11 ms  64.86.123.78
  9     *        *        *     Request timed out.
 10    32 ms    30 ms    28 ms  65-113-36-2.dia.static.qwest.net [65.113.36.2]
 11    30 ms    31 ms    30 ms  a184-87-144-170.deploy.akamaitechnologies.com [184.87.144.170]

Trace complete.

C:\>
```

The above two examples show first that long entries wrap and are hard to read. In the second one I reset my window width. You don't have to do this, but I right-clicked on the icon in the upper-left corner of the window and chose **Properties**.

Then I set the **Screen Buffer** and **Window Size** to **96** characters wide.

Note the three other tabs let you change other things like colors. In the third image, I set mine to yellow on blue.



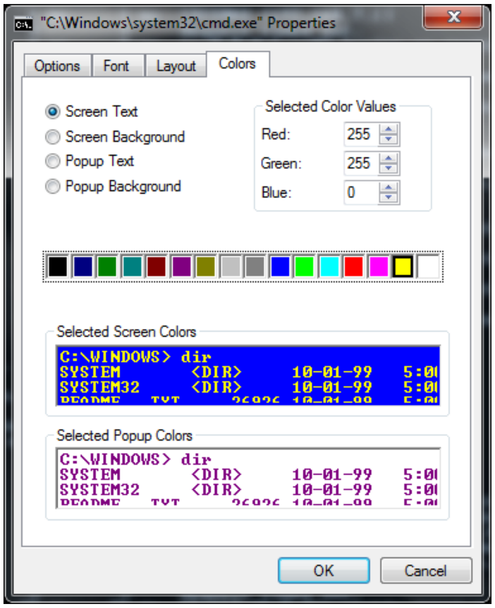


Screen Buffer Size
Width: 96
Height: 300

Window Size
Width: 96
Height: 51

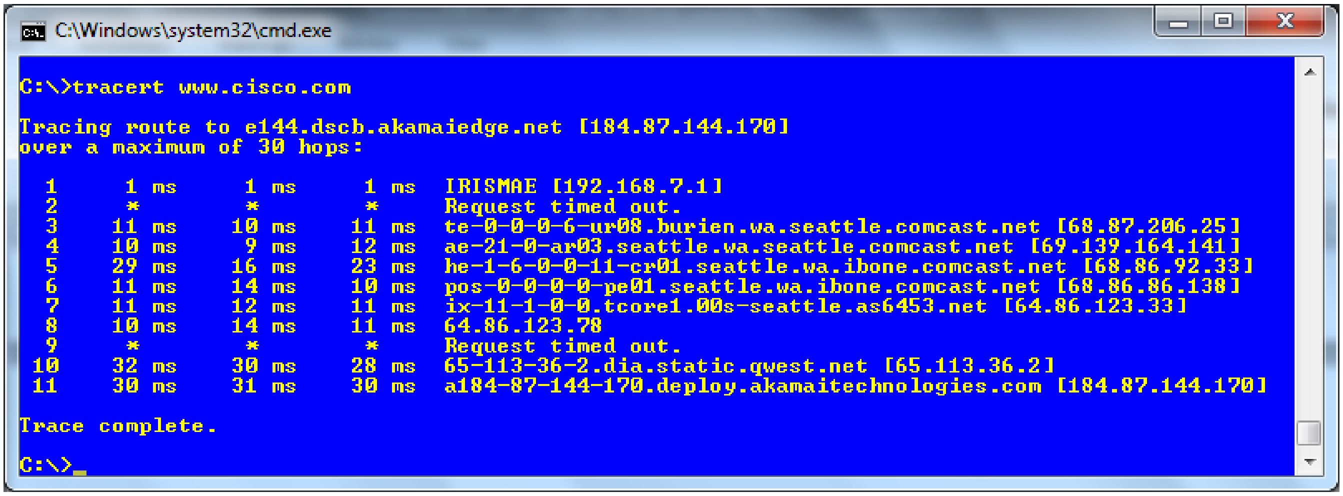
Window Position
Left: 233
Top: 12

☑ Let system position window


"C:\Windows\system32\cmd.exe" Properties
Options
Font
Layout
Colors
Selected Screen Colors
Selected Popup Colors
C:\WINDOWS> dir
SYSTEM <DIR> 10-01-99 5:0
SYSTEM32 <DIR> 10-01-99 5:0
OK
Cancel

● Screen Text
○ Screen Background
○ Popup Text
○ Popup Background

Selected Color Values
Red: 255
Green: 255
Blue: 0



```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [184.87.144.170]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  IRISMAE [192.168.7.1]
  2     *        *        *     Request timed out.
  3    11 ms    10 ms    11 ms  te-0-0-0-6-ur08.burien.wa.seattle.comcast.net [68.87.206.25]
  4    10 ms     9 ms    12 ms  ae-21-0-ar03.seattle.wa.seattle.comcast.net [69.139.164.141]
  5    29 ms    16 ms    23 ms  he-1-6-0-0-11-cr01.seattle.wa.ibone.comcast.net [68.86.92.33]
  6    11 ms    14 ms    10 ms  pos-0-0-0-0-pe01.seattle.wa.ibone.comcast.net [68.86.86.138]
  7    11 ms    12 ms    11 ms  ix-11-1-0-0.tcore1.00s-seattle.as6453.net [64.86.123.33]
  8    10 ms    14 ms    11 ms  64.86.123.78
  9     *        *        *     Request timed out.
 10    32 ms    30 ms    28 ms  65-113-36-2.dia.static.qwest.net [65.113.36.2]
 11    30 ms    31 ms    30 ms  a184-87-144-170.deploy.akamaitechnologies.com [184.87.144.170]

Trace complete.

C:\>_
```

Tracert is TCP/IP's abbreviation for **trace route**. The above figure shows the possible result when running **tracert www.cisco.com**.

The first line of output shows you the Fully Qualified Domain Name (FQDN)of the organization hosting cisco.com followed by the IP address – the address is hosted by Akamai, a large hosting firm.

So, we know that a DNS server could resolve the name to an IP address. Then there are listings of all routers (hops) the Tracert requests had to pass through to get to the destination.

The **IRISMAE** is the first router it hit – my router at my house, Iris is my granddaughter.

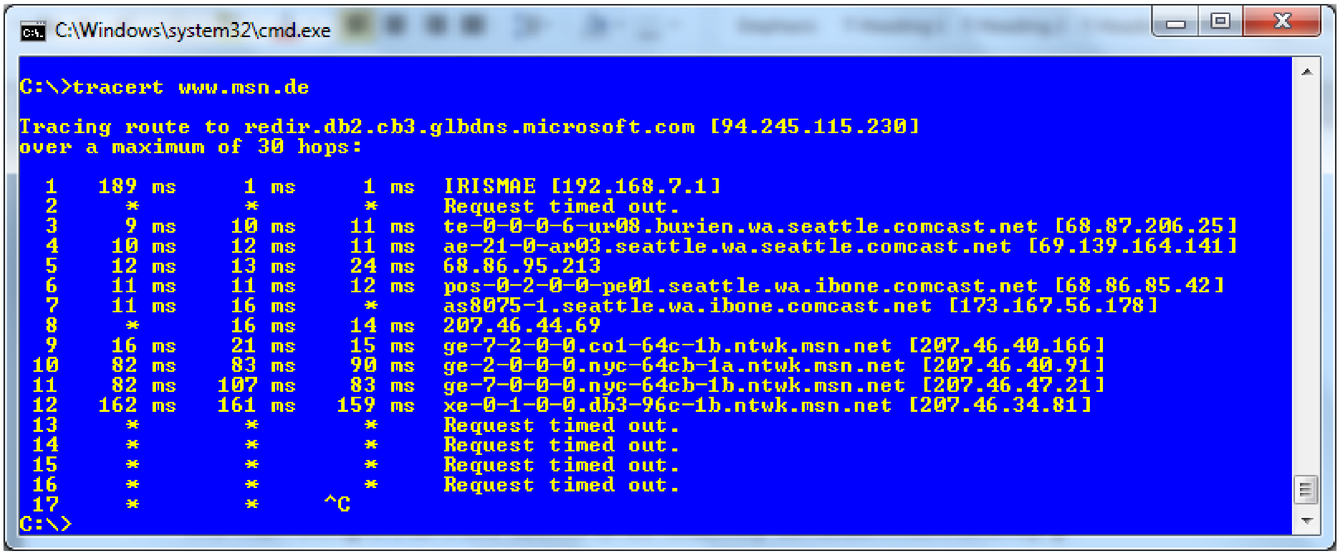
The **2nd and 9th routers** (hops) chose not to play with us – configured not to respond – but still passed the requests on to the next device. We'll solve the mystery on the 2nd in next exercise.

Routers 3-6 are Comcast (Xfinity) routers, so it is still on my ISP's network in Seattle.

Routers 7-10 got us to Akamai's edge router.

Tracert uses the same **echo** requests and replies as the **ping** command but in a slightly different way. You should see that Tracert contacted each router three times. By comparing the results, we can gauge the consistency of the route. Notice in the above example that there were relatively long delays after router 2 and 9, possibly due to congestion. The main thing is that there seems to be relatively consistent connectivity.

Each router represents a point where one network connected to another and your packet was forwarded through.



```
C:\>tracert www.msn.de

Tracing route to redir.db2.cb3.glbdns.microsoft.com [94.245.115.230]
over a maximum of 30 hops:

  1   189 ms     1 ms     1 ms  IRISMAE [192.168.7.1]
  2     *        *        *     Request timed out.
  3     9 ms    10 ms    11 ms  te-0-0-0-6-ur08.burien.wa.seattle.comcast.net [68.87.206.25]
  4    10 ms    12 ms    11 ms  ae-21-0-ar03.seattle.wa.seattle.comcast.net [69.139.164.141]
  5    12 ms    13 ms    24 ms  68.86.95.213
  6    11 ms    11 ms    12 ms  pos-0-2-0-0-pe01.seattle.wa.ibone.comcast.net [68.86.85.42]
  7    11 ms    16 ms     *     as8075-1.seattle.wa.ibone.comcast.net [173.167.56.178]
  8     *       16 ms    14 ms  207.46.44.69
  9    16 ms    21 ms    15 ms  ge-7-2-0-0.co1-64c-1b.ntwk.msn.net [207.46.40.166]
 10    82 ms    83 ms    90 ms  ge-2-0-0-0.nyc-64cb-1a.ntwk.msn.net [207.46.40.91]
 11    82 ms   107 ms    83 ms  ge-7-0-0-0.nyc-64cb-1b.ntwk.msn.net [207.46.47.21]
 12   162 ms   161 ms   159 ms  xe-0-1-0-0.db3-96c-1b.ntwk.msn.net [207.46.34.81]
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *      ^C
C:\>
```

Note: If you get a quite a few rows of stars, the destination device has probably been configured not to reply to PINGs. Press **[Ctrl]+c** to stop the command. Don’t be too quick though because it is not uncommon to get 3-4 rows of stars and then start again as it enters a different network.

Single stars indicate lost pings.

Look at the big jump in time at Router 12, what could that be? You have enough info to make to educated guesses: ____

Part 6

Try tracert on other domain names or IP addresses like Yahoo and record the results:

Example: www.cnn.com is at least 11 hops (routers) away

____

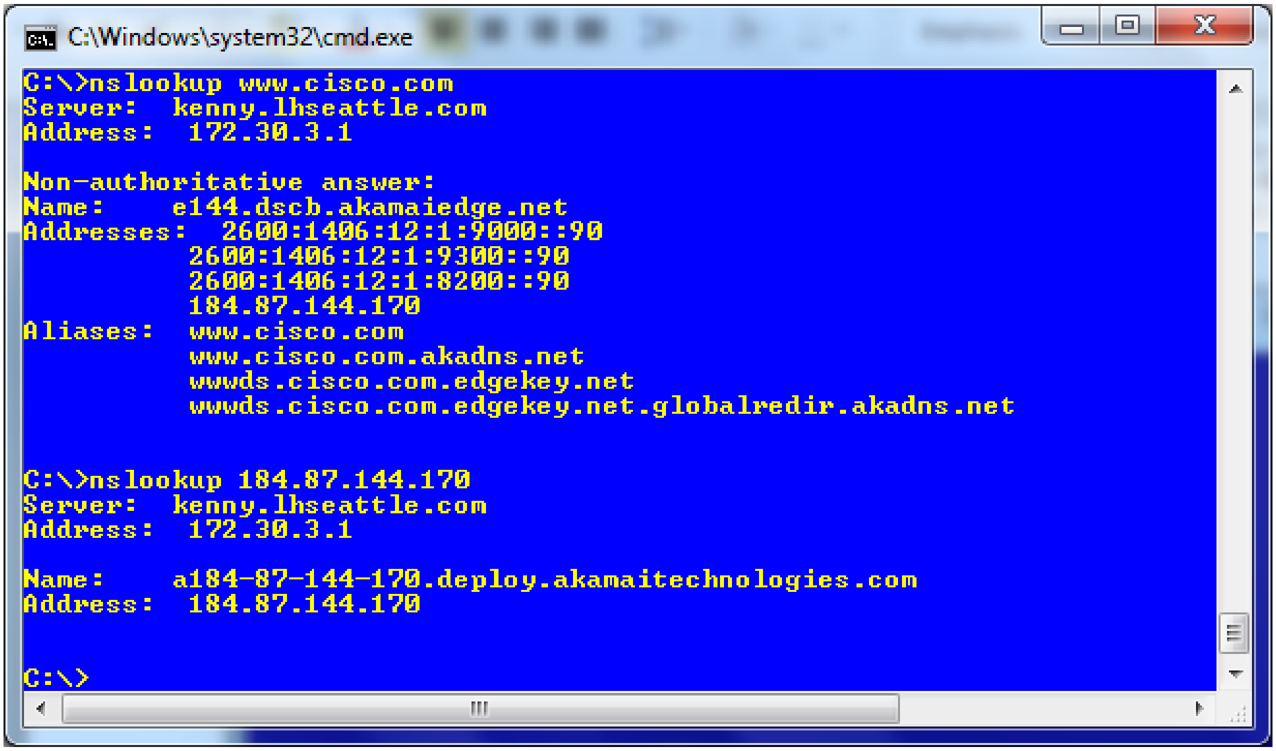
____

____

____

Part 7 – NSLOOKUP

In this next exercise, we will use the **nslookup** command, a DNS feature to find the IP address(es) for a domain name or any domain names associated with an IP address. Either way a domain name query packet is sent to a designated (or defaulted) DNS server for resolution. An example of each form:

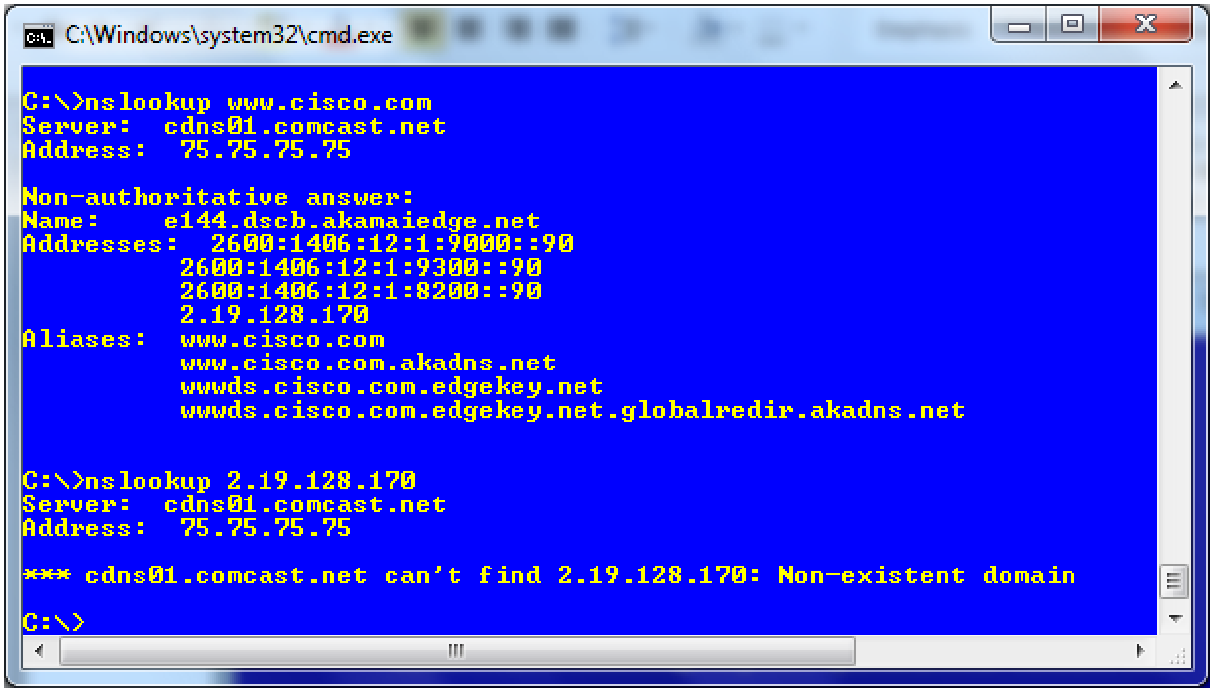


```
C:\>nslookup www.cisco.com
Server:  kenny.lhseattle.com
Address:  172.30.3.1

Non-authoritative answer:
Name:    e144.dscb.akamaiedge.net
Addresses:  2600:1406:12:1:9000::90
          2600:1406:12:1:9300::90
          2600:1406:12:1:8200::90
          184.87.144.170
Aliases:  www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net


C:\>nslookup 184.87.144.170
Server:  kenny.lhseattle.com
Address:  172.30.3.1

Name:    a184-87-144-170.deploy.akamaitechnologies.com
Address:  184.87.144.170


C:\>
```

NSLookup is supposed to help us find the owner of an IP address or domain name. Unfortunately, due to hackers using it to exploit networks – as compared to iSchool students who are engaged in learning – it often no longer works too well.

In the above example, the “Non-authoritative” means that cisco.com is not configured to let its DNS servers share that answer, but Akamai's DNS server knows and is sharing it with you. So, they have told us the name of the network at their site that uses that name – for Cisco, the addresses associated with it and any URLs it has for it (4).

When we nslookup on the IP address (the reverse of what we just did), it resolved back to Akamai, not Cisco because that is who owns that address.



```
C:\>nslookup www.cisco.com
Server:  cdns01.comcast.net
Address:  75.75.75.75

Non-authoritative answer:
Name:    e144.dscb.akamaiedge.net
Addresses:  2600:1406:12:1:9000::90
          2600:1406:12:1:9300::90
          2600:1406:12:1:8200::90
          2.19.128.170
Aliases:  www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net


C:\>nslookup 2.19.128.170
Server:  cdns01.comcast.net
Address:  75.75.75.75

*** cdns01.comcast.net can't find 2.19.128.170: Non-existent domain

C:\>
```

Note in line two it is Comcast, my ISP; that is making the request. Akamai gave us their info again, and the URLs but the address they gave us won't work for the second attempt. This is pretty common.

Note: Many searches by IP address will fail because of company security configurations.

In the command window, try: **nslookup ischool.uw.edu**

What is the IP address(es)? ____

Try the reverse on the IP address you got. You are trying to confirm it.

What is the Domain Name? ____

Try any domain names you like and record the IPs.

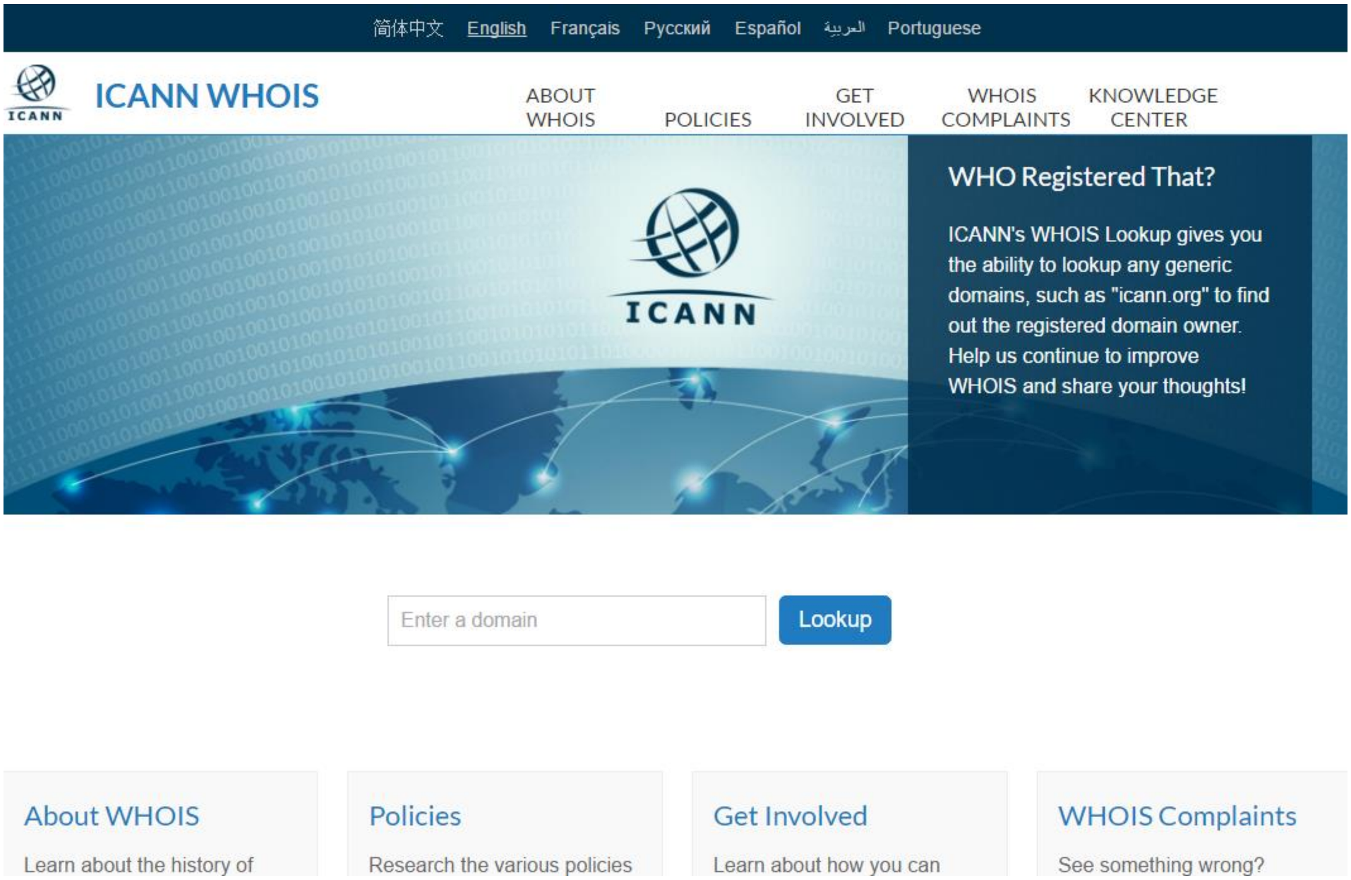
Part 8 – WHOIS

There is another way to learn more about a domain name or to determine if a particular domain name is registered. If not, it would probably be available to register and use. This process uses the **Whois** search service which can be performed by different online services with varying interests in helping you. You can Google whois and get many listings.

The **Internet Corporation for Assigned Names and Numbers (ICANN)** is the private-sector, non-profit corporation created in 1998 to assume responsibility for IP names. They are a public-benefit corporation with participants from all over the world dedicated to keeping the Internet secure, stable and interoperable.

Their site https://whois.icann.org/en amounts to going to the source, but due to their mission, they also run you through a couple of hurdles to avoid becoming a resource for hacker tools.

Go to https://whois.icann.org/en and look over the site for lots of information on whois and the organization itself.



WHO Registered That?

ICANN's WHOIS Lookup gives you the ability to lookup any generic domains, such as "icann.org" to find out the registered domain owner. Help us continue to improve WHOIS and share your thoughts!

Learn about the history of

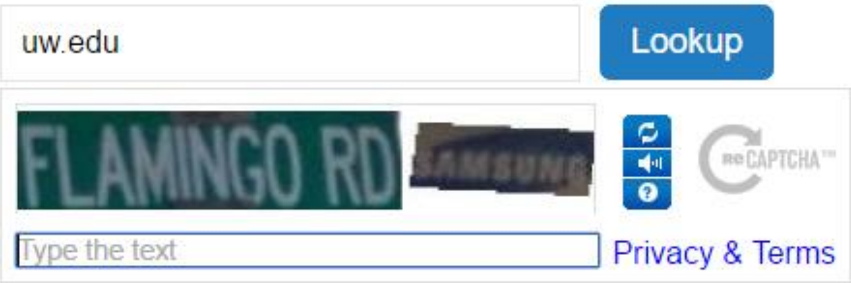
Research the various policies

Learn about how you can

See something wrong?

Type **uw.edu** in the **Enter a domain** box and click on **Lookup**.

You will be prompted with CAPTCHA to thwart automated (think hacking) tools.



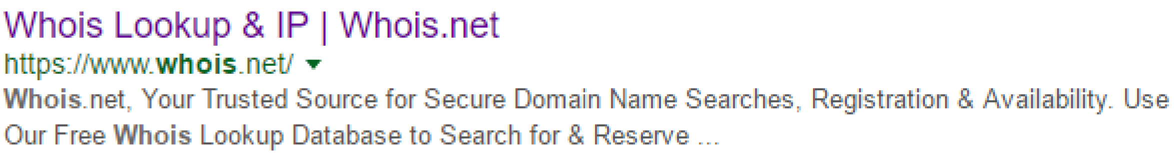
Make the appropriate entries. I found it not to be case sensitive, but it wants both items and any enclosed spaces.

You will get the entire **Raw WHOIS Record**. Look over the results. Notice the output is limited to information on your search target.

Now that you've done it the right way let's take a look at the other options.

Start by Googling **whois**. You will find many services including ICANN – most are name registry or hosting sites hoping to sell you services.

You can experiment with others but let's start with:

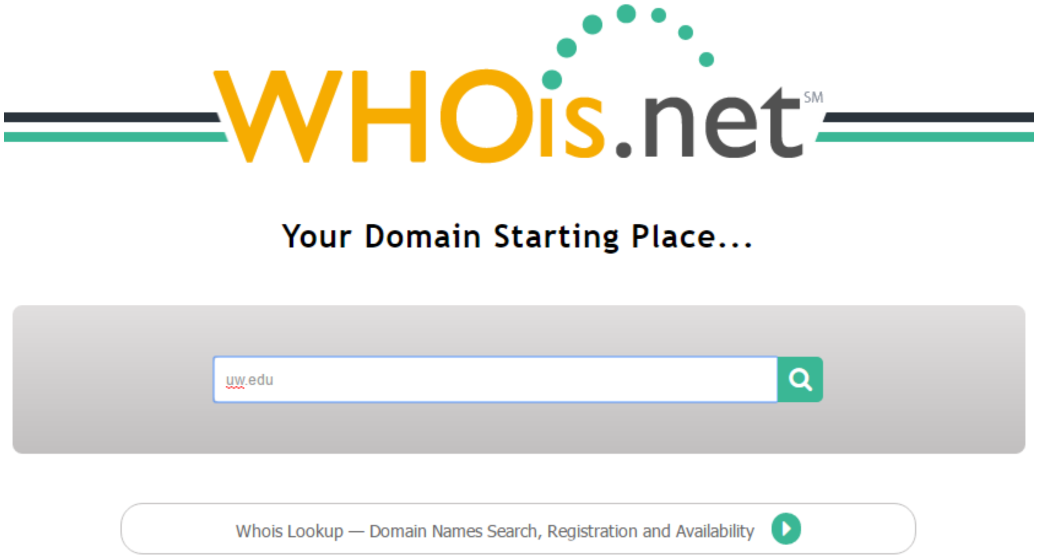


Whois Lookup & IP | Whois.net

https://www.**whois**.net/ ▾

Whois.net, Your Trusted Source for Secure Domain Name Searches, Registration & Availability. Use Our Free **Whois** Lookup Database to Search for & Reserve ...

If you select it you will get a screen like this:



WHOis.net℠

Your Domain Starting Place...

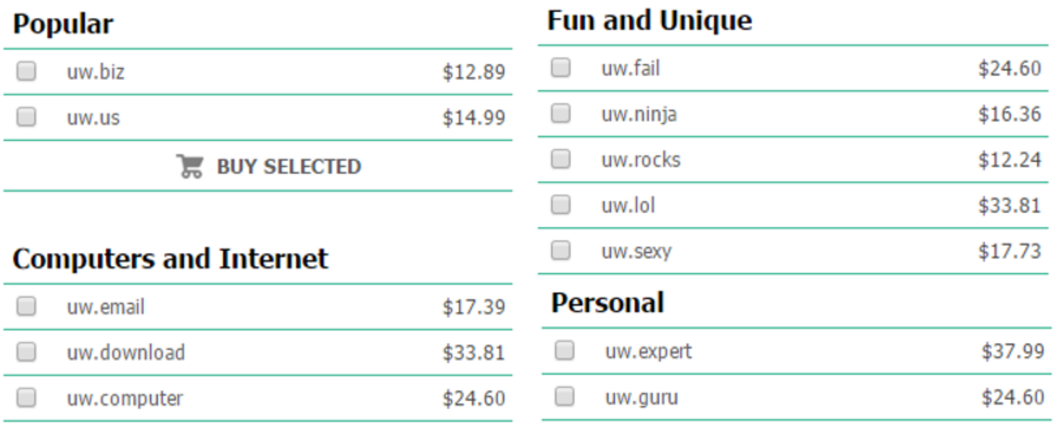
uw.edu

Whois Lookup — Domain Names Search, Registration and Availability

Type in **uw.edu** and press **Enter** and up comes much of the information you saw on ICANN's site, but not all usually. Note there was no CAPTCHA.

You can see when a domain was created, who owns it, who hosts it including foreign sites.

It does tell you the name is already registered. Then it goes on to offer you many similar names or variations of UW. Who might want a name so similar and why? What might you do with names like any of the following?



Popular

☐	uw.biz	$12.89
☐	uw.us	$14.99

BUY SELECTED

Computers and Internet

☐	uw.email	$17.39
☐	uw.download	$33.81
☐	uw.computer	$24.60

Fun and Unique

☐	uw.fail	$24.60
☐	uw.ninja	$16.36
☐	uw.rocks	$12.24
☐	uw.lol	$33.81
☐	uw.sexy	$17.73

Personal

☐	uw.expert	$37.99
☐	uw.guru	$24.60

Try looking up any other domain names on any service. Summarize your results.

I ran **boblarson.com** and **bla.com** (a domain I've owned since 1994). Sometimes you have to try twice to get a result – I can only speculate why.