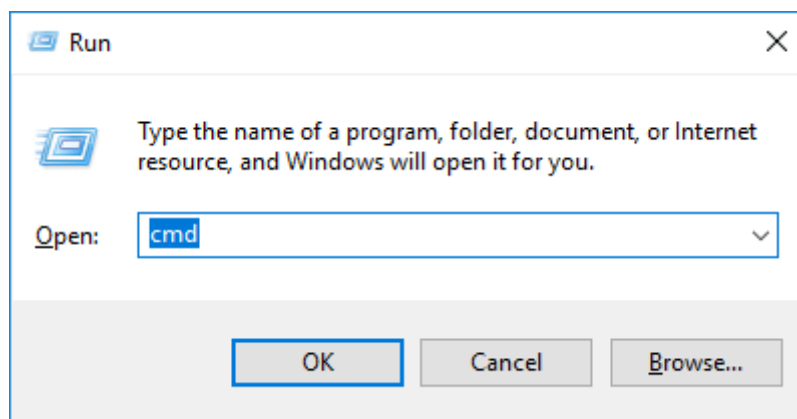


DNS Lab

The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates domain names meaningful for users to the numerical IP addresses needed for the purpose of locating computer services and devices worldwide. By providing a worldwide, distributed keyword-based redirection service, the Domain Name System is an essential component of the functionality of the Internet.

1. Open up the command prompt (In Windows, you can use WINDOWS KEY+R to open Run dialogue box and type **cmd**). You should see the following.



(note: Use up & down arrow keys to access recent commands entered in the command line.)

2. To see your current DNS settings, type **ipconfig /displaydns** and press Enter.

```
C:\Users\se10042310>ipconfig /displaydns

Windows IP Configuration

csi.gstatic.com
-----
Record Name . . . . . : csi.gstatic.com
Record Type . . . . . : 1
Time To Live . . . . . : 107
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 216.58.212.163

Record Name . . . . . : csi.gstatic.com
Record Type . . . . . : 1
Time To Live . . . . . : 107
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 172.217.17.99
```

3. To delete the entries, type **ipconfig /flushdns** and press Enter.

```
C:\Users\se10042310>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

4. To see your DNS settings again, type **ipconfig /displaydns** and press Enter.
(You should see blank records or you might get the message "Could not display the DNS Resolver Cache." as shown below).

```
C:\Users\se10042310>ipconfig /displaydns

Windows IP Configuration

Could not display the DNS Resolver Cache.

C:\Users\se10042310>
```

5. To perform a DNS lookup (from a laptop or outside the university), type **ping www.ulster.ac.uk** and press Enter. If you get no response then try step 6.

```
C:\Users\se10042310>ping www.ulster.ac.uk

Pinging www.ulster.ac.uk [192.195.43.223] with 32 bytes of data:
Reply from 192.195.43.223: bytes=32 time=1ms TTL=54
Reply from 192.195.43.223: bytes=32 time=1ms TTL=54
Reply from 192.195.43.223: bytes=32 time=1ms TTL=54
Reply from 192.195.43.223: bytes=32 time=1ms TTL=54

Ping statistics for 192.195.43.223:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

6. To perform a DNS lookup in the lab, type **ping 193.61.191.201** and press Enter

```
U:\>ping 193.61.191.201

Pinging 193.61.191.201 with 32 bytes of data:
Reply from 193.61.191.201: bytes=32 time<1ms TTL=255
Reply from 193.61.191.201: bytes=32 time=3ms TTL=255
Reply from 193.61.191.201: bytes=32 time=2ms TTL=255
Reply from 193.61.191.201: bytes=32 time<1ms TTL=255

Ping statistics for 193.61.191.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

Note: Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network. It measures the round-trip time for messages sent from the originating host to a destination computer that are echoed back to the source. The name comes from active sonar terminology that sends a pulse of sound and listens for the echo to detect objects under water.

Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP echo reply. The program reports errors, packet loss, and a statistical summary of the results, typically including the minimum, maximum, the mean round-trip times, and standard deviation of the mean. The command-line options of the ping utility and its output vary between the numerous implementations. Options may include the size of the payload, count of tests, limits for the number of network hops (TTL) that probes traverse, and interval between the requests.

To see your DNS settings again, type **ipconfig /displaydns** and press Enter.

(you will see different records than mine. I see Dropbox because that is running in the background on my machine. I also see a record for www.getpaint.net which is interesting as I never visited that site today but I am using that image editing program to edit these images. It seems the program automatically requested that site perhaps for an update check. Tools like this can help you see what is happening on your network.)

```
C:\Users\se10042310>ipconfig /displaydns

Windows IP Configuration

        beacon.dropbox.com
        -----
        Record Name . . . . . : beacon.dropbox.com
        Record Type . . . . . : 5
        Time To Live . . . . . : 50
        Data Length . . . . . : 8
        Section . . . . . : Answer
        CNAME Record . . . . . : beacon.v.dropbox.com

        Record Name . . . . . : beacon.v.dropbox.com
        Record Type . . . . . : 1
        Time To Live . . . . . : 50
        Data Length . . . . . : 4
        Section . . . . . : Answer
        A (Host) Record . . . . : 162.125.34.129

        www.getpaint.net
        -----
        Record Name . . . . . : www.getpaint.net
        Record Type . . . . . : 1
        Time To Live . . . . . : 3394
        Data Length . . . . . : 4
        Section . . . . . : Answer
        A (Host) Record . . . . : 208.112.63.123
```

7. If you scroll down your list, you should see a DNS record for www.ulster.ac.uk or whichever site or ip address you pinged that includes the IP address and other information. Another field in the DNS cache is a TTL value, which is different from the TTL in an IP packet. This DNS TTL value is sent by the DNS server maintaining the www.ulster.ac.uk record. It is measured in seconds and tells your DNS client how long to cache the DNS record as a safeguard against clients holding on to DNS records whose IP addresses might have changed.

```

www.ulster.ac.uk
-----
Record Name . . . . . : www.ulster.ac.uk
Record Type . . . . . : 1
Time To Live . . . . . : 74470
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 192.195.43.223

Record Name . . . . . : www.ulster.ac.uk
Record Type . . . . . : 1
Time To Live . . . . . : 74470
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 192.195.43.123

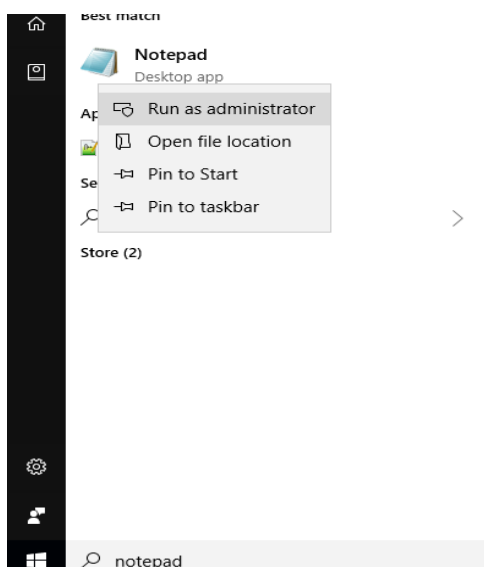
```

On occasion you will need to edit the hosts file on a machine. Sometimes because of an attack and others so that you can simply and freely control access to websites and network traffic. Hosts files have been in use since ARPANET. They were used to resolve hosts names before DNS. hosts files would be massive documents used to aide the network name resolution. Microsoft kept the hosts file alive in Windows networking which is why it varies very little whether used in Windows, macOS, or Linux. The syntax stays mostly the same across all platforms. Most hosts files will have several entries for loopback. We can use that for the basic example for the typical syntax. The first part will be the location to redirect the address to, the second part will be the address that you will want to redirect, and the third part is the comment. They can be separated by a space, but for ease of reading are typically separated by one or two tabs.

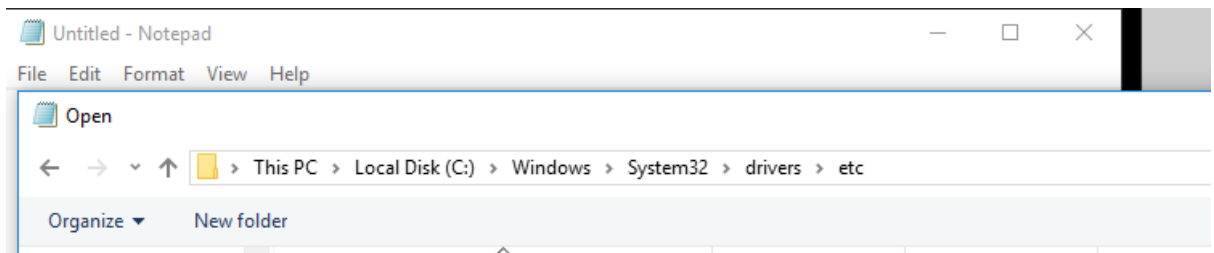
127.0.0.1 localhosts #loopback

Next, we look at accessing the hosts files in Windows.

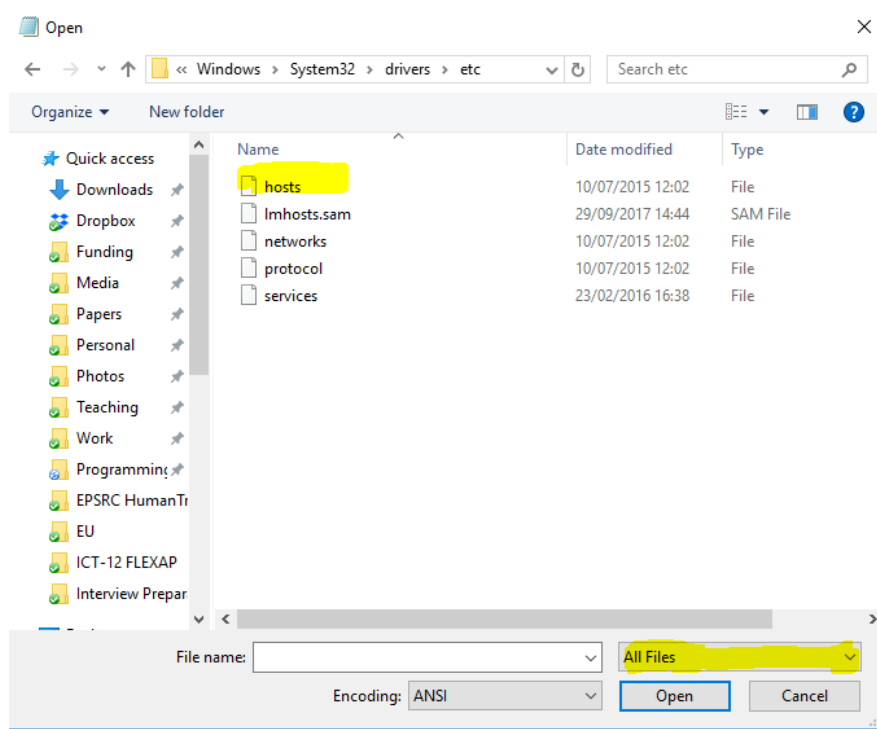
8. To open your computer's Hosts file, run Notepad as administrator. Easiest way is to press the Windows key and then type notepad in bottom left. Select notepad and right click and then select "Run as administrator" in bottom taskbar area as shown below.



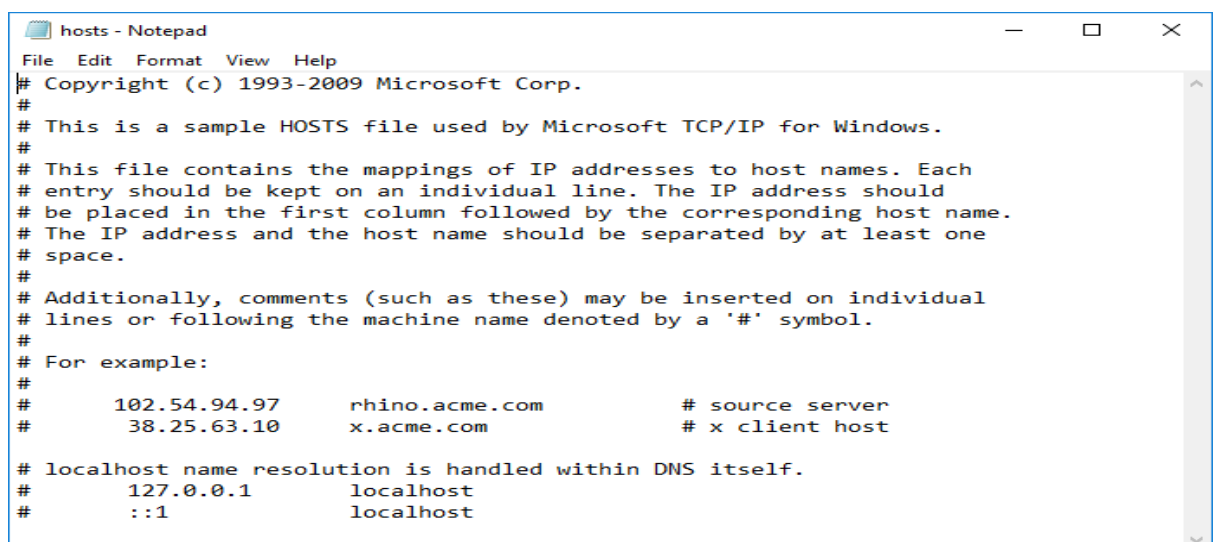
9. In the Open dialog box, navigate to C:\Windows\System32\Drivers\Etc.



10. In the File type drop-down list, **click All Files**. Double-click the **hosts** file to open it.



11. You should now have a hosts file open with various settings. Mine is shown below.



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97      rhino.acme.com      # source server
#      38.25.63.10      x.acme.com          # x client host
#
# localhost name resolution is handled within DNS itself.
#      127.0.0.1        localhost
#      ::1              localhost
```

12. After the *last line in the file*, type **192.195.43.123 university**, and then save the file and exit Notepad.

```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1            localhost
|
192.195.43.123 university
```

13. At the command prompt, type **ipconfig /displaydns** to see that the entry is in your DNS cache.

```
C:\Users\se10042310>ipconfig /displaydns

university
-----
No records of type AAAA

university
-----
Record Name . . . . . : university
Record Type . . . . . : 1
Time To Live . . . . . : 0
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 192.195.43.123

123.43.195.192.in-addr.arpa
-----
Record Name . . . . . : 123.43.195.192.in-addr.arpa.
Record Type . . . . . : 12
Time To Live . . . . . : 0
Data Length . . . . . : 8
Section . . . . . : Answer
PTR Record . . . . . : university
```

14. Type **ping university** and press Enter.

```
C:\Users\se10042310>ping university

Pinging university [192.195.43.123] with 32 bytes of data:
Reply from 192.195.43.123: bytes=32 time=2ms TTL=54
Reply from 192.195.43.123: bytes=32 time=1ms TTL=54
Reply from 192.195.43.123: bytes=32 time=1ms TTL=54
Reply from 192.195.43.123: bytes=32 time=2ms TTL=54

Ping statistics for 192.195.43.123:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\se10042310>
```

15. Delete the DNS cache again by typing **ipconfig /flushdns** and press Enter.

```
C:\Users\se10042310>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

16. Display your DNS cache by typing **ipconfig /displaydns** and press Enter.

```
client.dropbox.com
-----
Record Name . . . . . : client.dropbox.com
Record Type . . . . . : 5
Time To Live . . . . . : 37
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . . : client.dropbox-dns.com

Record Name . . . . . : client.dropbox-dns.com
Record Type . . . . . : 1
Time To Live . . . . . : 37
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 162.125.64.3

university
-----
No records of type AAAA

university
-----
Record Name . . . . . : university
Record Type . . . . . : 1
Time To Live . . . . . : 0
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 192.195.43.123
```

Notice that the university entry remains in the cache because the Hosts file data always stays in the cache. Some others like Dropbox may appear as they are constantly probing sites in the background and thus filling the DNS cache table anew each time.

17. Type **nslookup www.ulster.ac.uk** and press Enter.

```
C:\Users\se10042310>nslookup www.ulster.ac.uk
Server:      scis5.scis.ulster.ac.uk
Address:     193.61.191.105

Non-authoritative answer:
Name:        www.ulster.ac.uk
Addresses:   192.195.43.223
             192.195.43.123
```

Your DNS server's name and IP address are displayed, along with the name and IP address of www.ulster.ac.uk. You use Nslookup to look up a host's IP address without actually communicating with it.

18. Type **nslookup** and press Enter.

```
C:\Users\se10042310>nslookup
Default Server:  scis5.scis.ulster.ac.uk
Address:  193.61.191.105
>
```

You should now have entered Nslookup's interactive mode. You should see an arrow prompt.

19. Type **www.google.com** and press Enter.

```
> www.google.com
Server:  scis5.scis.ulster.ac.uk
Address:  193.61.191.105

Non-authoritative answer:
Name:    www.google.com
Addresses:  2a00:1450:4007:80a::2004
           216.58.204.100
>
```

Here the address is returned along with one or more aliases (other names that `www.google.com` goes by). The `www.google.com` page can be reached by several different IP addresses, and the addresses are often returned in a different order so that a different server is used each time, which is called load balancing. Nslookup is also used to do reverse lookups, in which the IP address is given and the hostname is returned.

If you are ever concerned that your DNS server is not working correctly, you can test it with Nslookup and compare the results of your DNS server with the results from another server, such as Google's.

The biggest news story for many years relating to DNS was when Cloudflare announced a [new privacy-friendly 1.1.1.1 public DNS service](#). It appeared in many news sites. This is the future for DNS.