**Homework 2:** DNS and dig/nslookup Utilities

This wireshark lab is to be used in conjunction with the use of the ‘dig’ utility[[1]](#footnote-1) (Linux/Mac) and nslookup (Windows)[[2]](#footnote-2). Note: ‘dig’ is the preferred tool and is available for download on Windows as well. See References for documentation.

Run the ‘dig’/’nslookup’ network utility to look up IP addresses for the following hostnames while wireshark is running on your WiFI interface and capture the wireshark output in a file.:

[www.njit.edu](http://www.njit.edu).

afsconnect1.njit.edu.

[www.google.com](http://www.google.com)

[www.amazon.com](http://www.amazon.com)

njit.edu. (in this case look up type NS records and not type A records)

Also, run dig on the AFS machine (afsconnect1.njit.edu) for the above hostnames as well.

Both dig and nslookup are using the DNS protocol to reach a DNS server to resolve the hostnames into one or more IPv4 and/or IPv6 addresses.

Examine the corresponding wireshark trace for each of the above lookups, along with the dig/nslookup output:

1. What packet # corresponds to the DNS request? What packet # corresponds to the DNS response? What would you look for in the DNS or other protocol headers to determine what is a DNS request and what is a DNS response?

1,3,5,7

1. Is the answer from the authoritative server or not? What would you look at in the DNS protocol header to determine this?

Answer is in the authoritative, and will show up as 1 in the Authoritative

1. What does authoritative mean?

Authoritative servers are the organization’s own servers, providing authoritative hostname to IP mappings for organizations’ named hosts.

1. What type of resource records are used to query for IPv4 addresses?

A type

1. What type of resource records are used to query for name servers responsible for a particular domain?
2. How many IP addresses are returned in the DNS response?

1

It is possible that a host may have multiple IP addresses, meaning multiple type A records would be returned in the DNS response for that hostname. The answer is thus just a count of the type A records returned for the hostname in the answer section of the DNS response.

1. In some cases, the answer returns a CNAME resource record. What is the purpose of this resource record type?

The DNS server will continue the retrying the lookup with the new name

1. What type of resource records are contained in the Authority section of the response? What information do these records contain?

NS: Name Server Lookup, name server addresses

1. What type of resource records are contained in the Additional section of the response? What information do these records contain?

A type which contains ip address

References:

1. <https://linux.die.net/man/1/dig> -- documentation on *dig*
2. <https://technet.microsoft.com/en-us/library/bb490950.aspx> – documentation on nslookup
3. <https://www.lifewire.com/what-is-nslookup-817516> -- documentation on nslookup
4. <https://blog.thesysadmins.co.uk/nslookup-common-usage-examples.html> -- documentation on nslookup
5. <https://help.dyn.com/how-to-use-binds-dig-tool/> --- help on how to use *dig* with examples and download instructions for Windows
6. <http://nil.uniza.sk/linux-howto/how-install-dig-dns-tool-windows-10> -- more detailed instructions for Windows download

1. The manual page for dig (Linux) is https://linux.die.net/man/1/dig [↑](#footnote-ref-1)
2. Documentation for nslookup: <https://technet.microsoft.com/en-us/library/bb490950.aspx> [↑](#footnote-ref-2)