50.005 Computer System Engineering
Lab 7: DNS

Joel Huang, 1002530

April 12, 2018

1 DNS Basics

1. 18.26.0.122
2. CNAME refers to canonical name, which is an alias that points to the actual domain. For example, thyme.lcs.mit.edu is a CNAME record that points to mercury.lcs.mit.edu. When an A record lookup for thyme occurs, the resolver will detect the CNAME record and restart the check for mercury and return 18.26.0.122.
3. 1800s
4. 'ai' - no IP address, 'ai.' - 209.59.119.34
5. From man pages, +domain sets the search list to contain a single domain, as if specified in a domain directive in /etc/resolv.conf, and enable search list processing as if the +search option were given. +domain searches for a specified single domain, in this case 'ai' resolved to 'ai.mit.edu', while 'ai.' resolved to Anguilla's domain registrar at 209.59.119.34.
6. dig edu to get a.edu-servers.net, then dig @a.edu-servers.net lirone.csail.mit.edu +norecurse
7. dig @a.edu-servers.net lirone.csail.mit.edu +norecurse dig @asia2.akam.net lirone.csail.mit.edu +norecurse dig @auth-ns1.csail.mit.edu lirone.csail.mit.edu +norecurse Which gives an A record of 128.52.129.186
8. dig www.ns.sg +norecurse gave no answer section, hence it was not cached. It took 4ms
9. 8ms
10. 4ms. The cache served its purposed as it produced an answer section which means the TTL has not expired, and the query was completed within a shorter time.

2 Wireshark

1. UDP
2. Port 53 and source port 57763
3. 192.168.2.11, they are not the same.
4. The second DNS query message is a recursive DNS query to update-keepalive.mcafee.com, which contains no answers.
5. There are 2 answers, one CNAME record pointing to updatekeepalive.glb.mcafee.com and the corresponding A record with address 161.69.12.13
6. The destination IP address of the SYN packet is 161.69.12.13, which is the IP address of updatekeepalive.glb.mcafee.com.