Wireshark Lab: Getting Started

Ethan Fison, Zan Montieth

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server
    - 58.229.6.225
2. Run nslookup to determine the authoritative DNS servers for a university in Europe.
    - dns0.ox.ac.uk internet address = 129.67.1.190
    - dns1.ox.ac.uk internet address = 129.67.1.191
    - dns2.ox.ac.uk internet address = 163.1.2.190
3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?
    - We recieved Query refused for all our attempted connections
4. Locate the DNS query and response messages. Are then sent over UDP or TCP?
    - TCP
5. What is the destination port for the DNS query message? What is the source port of DNS response message
    - TCP
        - destination is port 443
        - source port is 58818
    - DNS
        - destination port is 53
        - source port is 60209
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
    - 52.203.151.232
    - 192.168.0.1
    - They are not the same.
7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
    - standard
    - no
8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
    - 1 answer
    - they each have the
    - name of host
    - the type of address
    - a class
    - the TTl
    - data length
    - IP address
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
    - they do match

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?
    - no
11. What is the destination port for the DNS query message? What is the source port of DNS response message?
    - destination port is 53
    - source port is 52
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
    - 192.168.0.1
    - which is our local dns server
13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"
    - Query type is a standard query of type a
    - there are no answers
14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain
    - 3 answers were provided
        - From mit.edu sending alias name to mit.edu.edgekey.net
        - From mit.edu.edgekey.net sending alias name to e9566.dscb.akamaiedge.net
        - each answer contains name, type, class, TTL, data length, and either cname or address
15. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server
    - the dns query message was sent to 192.168.0.1
    - which is our local dns server
16. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
    - query type of NS
    - message does not contain any answers
17. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?
    - mit.edu nameserver = eur5.akam.net
    - mit.edu nameserver = use2.akam.net
    - mit.edu nameserver = use5.akam.net
    - mit.edu nameserver = usw2.akam.net
    - mit.edu nameserver = asia1.akam.net
    - mit.edu nameserver = asia2.akam.net
    - mit.edu nameserver = ns1-37.akam.net
    - mit.edu nameserver = ns1-173.akam.net
    - it does provide the ip addresses
18. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?
    - 192.168.0.1

> we had to use asia1.akam.net because bitsy.mit.edu does not exsist

21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"

```
- standard type a
- no answers
```

22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain
    - one answer is the ip to connect to
    - then no answers because connection refused