Daniel McDonough (dmcdonough)
Lab 2 9/11

Q1.

nslookup www.nintendo.co.jp

Output:

```
    Server:       127.0.1.1
    Address:      127.0.1.1#53

    Non-authoritative answer:
    www.nintendo.co.jp  canonical name = www.nintendo.co.jp.edgekey.net.
    www.nintendo.co.jp.edgekey.net  canonical name = e5192.g.akamaiedge.net.
    Name:   e5192.g.akamaiedge.net
    Address: 173.222.102.223
```

Q2.

nslookup -type=NS www.univ.ox.ac.uk

Output:

```
      Server:           127.0.1.1
      Address:    127.0.1.1#53

      Non-authoritative answer:
      *** Can't find www.univ.ox.ac.uk: No answer

      Authoritative answers can be found from:
      ox.ac.uk
      origin = nighthawk.dns.ox.ac.uk
      mail addr = hostmaster.ox.ac.uk
      serial = 2018091264
      refresh = 3600
      retry = 1800
      expire = 1209600
      minimum = 900
```

Q3(UPDATED). nslookup mail.yahoo.com 209.244.0.3

Output:

```
            Server:           209.244.0.3
            Address:    209.244.0.3#53

            Non-authoritative answer:
            mail.yahoo.com    canonical name = fd-geoycpi-uno.gycpi.b.yahoodns.net.
            Name: fd-geoycpi-uno.gycpi.b.yahoodns.net
            Address: 69.147.92.11
            Name: fd-geoycpi-uno.gycpi.b.yahoodns.net
            Address: 69.147.92.12
```

Start of Part1.pcapng

Q4. Sent Over UDP

Q5. Source port was 42193

Q6. The query was sent to Dst: 130.215.11.86
    The local DNS IP shown by ifconfig -a: 130.215.11.86
    They are the same!

Q7. The query type was sent as both type A and type AAAA, but neither contained no answers

Q8. The response for both type A and type AAAA response had 3 answers. Which contained:

  www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
  www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2400:cb00:2048:1::6814:55
  www.ietf.org.cdn.cloudflare.net: type AAAA, class IN, addr 2400:cb00:2048:1::6814:155

where the type's changed per type of resoponse.

Q9. The following TCP was sent to Dst: 130.215.11.86 which is the same IP as above

Q10. No the images are loaded from www.ietf.org

Start of Part2.pcapng

Q11. Dst of Query Port: 53
     Src of Response Port: 42193

Q12. Dst: 130.215.11.86 which is the same as my local dns

Q13. The query was of type A, and contained only the query (no answers)

Q14. The Response contained 3 answers:
  www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
  www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
  e9566.dscb.akamaiedge.net: type A, class IN, addr 23.14.144.128

Q15. See Q15.png

Start of Part3.pca.png
Q16. The Query was sent to 130.215.11.86 which is still my default DNS Server

Q17. The Response is of type CNAME. And contains 2 answers:
    www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net

Q18. The nameserver responses were:
        www.mit.edu.edgekey.net
        e9566.dscb.akamaiedge.net
      The responses did not contain the IP address

Q19. See Attached Q19.png

Start of Part4(updated).pcapng
Using nslookup www.aiit.or.kr 209.244.0.3

Q20. The query was sent to Dst: 209.244.0.3 which is not my local DNS but instead the second input of the nslookup command

Q21. Type A with no answers

Q22. The response contained 1 answer:
www.aiit.or.kr: type A, class IN, addr 58.229.6.225

Q23. See Attached Q23(updated).png