Part 1:

1. Identify a DNS interaction (query and response) in the trace.
2. Take screenshots of the query and response messages. (Or filter your trace so that only the request and response are visible, then save a copy of your trace file with **just those packets**.)
3. What transport layer protocol does DNS run over in this example? Explain why you think DNS runs over this protocol (answer in terms of the services DNS requires from the transport layer).
    a. Data: Coloring rule name and string User Datagram Protocol, Src Port: 55400, Dst Port: 53. It runs on UDP because of its low latency and small message size.
4. Summarize the contents of the query message.
    a. how many questions are contained in this message?
        i. 1
    b. what type of query is this?
        i. type HTTPS, class IN
    c. what flags are set?
        i. Flags: 0x0100 Standard query = Recursion desired
    d. what data is in the body of the message?
        i. It gave one ip address to send the data to and one authority name server (AWS)
5. Summarize the contents of the response message.
    a. how many responses does this message contain?
        i. 1
    b. identify the (name, TTL, type, class, value) tuple for each response.
        i. cloud.malwarebytes.com: type SOA, class IN, mname ns-2046.awsdns-63.co.uk
    c. what flags are set?
        i. Flags: 0x8180 Standard query response, No error

Part 2

1. _
    a.

```
❯ resolvectl status
Global
         Protocols: +LLMNR +mDNS -DNSOverTLS DNSSEC=no/unsupported
  resolv.conf mode: foreign
Fallback DNS Servers: 9.9.9.9#dns.quad9.net 2620:fe::9#dns.quad9.net
                      1.1.1.1#cloudflare-dns.com
                      2606:4700:4700::1111#cloudflare-dns.com
8.8.8.8#dns.google
                      2001:4860:4860::8888#dns.google
```

```
          DNS Domain: carleton.edu

Link 2 (wlan0)
    Current Scopes: DNS LLMNR/IPv4 LLMNR/IPv6 mDNS/IPv4 mDNS/IPv6
         Protocols: +DefaultRoute +LLMNR +mDNS -DNSOverTLS
DNSSEC=no/unsupported
Current DNS Server: 137.22.1.6
       DNS Servers: 137.22.1.7 137.22.1.6
        DNS Domain: carleton.edu
     Default Route: yes
```

   b. 2
   c. Carleton College 137.22.1.6

2. _
   a. _

```
❯ dig detect-remediate.cloud.malwarebytes.com

; <<>> DiG 9.20.15 <<>> detect-remediate.cloud.malwarebytes.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34733
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 4, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;detect-remediate.cloud.malwarebytes.com. IN A

;; ANSWER SECTION:
detect-remediate.cloud.malwarebytes.com. 17 IN A 98.89.234.153
detect-remediate.cloud.malwarebytes.com. 17 IN A 98.88.154.173
detect-remediate.cloud.malwarebytes.com. 17 IN A 98.89.67.191
detect-remediate.cloud.malwarebytes.com. 17 IN A 54.144.203.126

;; AUTHORITY SECTION:
cloud.malwarebytes.com. 432     IN      NS      ns-902.awsdns-48.net.
cloud.malwarebytes.com. 432     IN      NS      ns-1289.awsdns-33.org.
cloud.malwarebytes.com. 432     IN      NS      ns-440.awsdns-55.com.
cloud.malwarebytes.com. 432     IN      NS      ns-2046.awsdns-63.co.uk.

;; ADDITIONAL SECTION:
ns-440.awsdns-55.com.   22877   IN      A       205.251.193.184
```

```
;; Query time: 90 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Nov 10 13:38:14 CST 2025
;; MSG SIZE  rcvd: 285
```

b. Questions from part 1
   i. There is 1 question
   ii. Internet class, A record
   iii. flags: qr rd ra
   iv. The content gives the ipv4 address for malwarebytes and says the DNS Authority is from AWS

c. Both were a part of the internet class while the wireshark it was type HTTPS and dig gave A record. Dig gave more ip addresses and name servers compared to wireshark.

3. Add +trace
   a. Trace:

```
; <<>> DiG 9.20.15 <<>> detect-remediate.cloud.malwarebytes.com +trace
;; global options: +cmd
.                       245281  IN      NS      k.root-servers.net.
.                       245281  IN      NS      i.root-servers.net.
.                       245281  IN      NS      f.root-servers.net.
.                       245281  IN      NS      b.root-servers.net.
.                       245281  IN      NS      c.root-servers.net.
.                       245281  IN      NS      l.root-servers.net.
.                       245281  IN      NS      h.root-servers.net.
.                       245281  IN      NS      e.root-servers.net.
.                       245281  IN      NS      m.root-servers.net.
.                       245281  IN      NS      a.root-servers.net.
.                       245281  IN      NS      j.root-servers.net.
.                       245281  IN      NS      g.root-servers.net.
.                       245281  IN      NS      d.root-servers.net.
.                       313098  IN      RRSIG   NS 8 0 518400
20251124050000 20251111040000 61809 .
R9kC1ovDDzMbmNj4yZys8xowO4Vs/Ur8SmdL+P2V/m7OJB8AZZhBZJK1
xfiu4s+8O0ntX3+vl3j/G1BNkoZ0bVLXuh7bnAuFj7/VXNvPJctEJp5m
nbQIGktI80KcLe0OK9Sq+Hk4vqKq283VqkHJqxMl0l5cpwy+t8cV/Jju
LOnVCmKluuYES2zVfseHTH8O/ewI34mNrgce2iiWI0If/EqDEKxSe/wz
9M7cksUVvjm0mjECjL1XjtSVeJTUs7AuxkO1CysyAqvHwir/cJCTP2mF
I5jyy/eRulq0FQZF1pRaFbm7zX2y3nxztqmsu49Rs0M/y3Qwq3MWY/P3 ioKIMw==
;; Received 1125 bytes from 127.0.0.53#53(127.0.0.53) in 5 ms

;; UDP setup with 2001:500:12::d0d#53(2001:500:12::d0d) for
```

```
detect-remediate.cloud.malwarebytes.com failed: network unreachable.
;; no servers could be reached
;; UDP setup with 2001:500:12::d0d#53(2001:500:12::d0d) for
detect-remediate.cloud.malwarebytes.com failed: network unreachable.
;; no servers could be reached
;; UDP setup with 2001:500:12::d0d#53(2001:500:12::d0d) for
detect-remediate.cloud.malwarebytes.com failed: network unreachable.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
com.                    86400   IN      DS      19718 13 2
8ACBB0CD28F41250A80A491389424D341522D946B0DA0C0291F2D3D7 71D7805A
com.                    86400   IN      RRSIG   DS 8 1 86400 20251126210000
20251113200000 61809 .
3M7cgfdaZI+Ln4WBRYM45kQip/vbUSXu8IL/XdIiF7ceBqVXJ4Lgk8fA
2tJqgyknBSDX4E1y9EQbi0CckfdQsT4FUZR9aU+q0GczdVA1QSgV7dlC
VjppnL3/gOAfs8tnQ2abY1utiiTdurztci92M4hVAMcpTApxS+Zkh7/d
mM7O77Lb9dd0XqluQkZ05bu+iDzTCACS/7HzmAT8HWhBB+wlNIkjiqvX
tuP9j3ANYH9OqLwUvp3gtuyBY3eeDdzFHZAtNPAoSwrQ/q41nmEUjKTA
5X3cHqAJ8NFLHL0Hhtin5kdcMNwyHHgJLH0YNC/0XGvxUjrLKirhcxZJ v/+16Q==
;; Received 1199 bytes from 199.7.91.13#53(d.root-servers.net) in 5 ms

malwarebytes.com.       172800  IN      NS      ns-722.awsdns-26.net.
malwarebytes.com.       172800  IN      NS      ns-416.awsdns-52.com.
malwarebytes.com.       172800  IN      NS      ns-2045.awsdns-63.co.uk.
malwarebytes.com.       172800  IN      NS      ns-1460.awsdns-54.org.
malwarebytes.com.       86400   IN      DS      53272 13 2
A085590E0AA9ED4DFCF93CBC9F84C77A65930E1637C36C892A9C31C1 2D729989
malwarebytes.com.       86400   IN      RRSIG   DS 13 2 86400
20251118012230 20251111001230 46539 com.
g8R4DZhriKNqDy+uI5mNe/ZWlhkB4sHA61/vQJo+qYwWNbjpDPSBxv1Z
5kStMlpIOYdnvjJ3IqvShe9PLwAfdA==
;; Received 368 bytes from 192.33.14.30#53(b.gtld-servers.net) in 9 ms
;; UDP setup with 2600:9000:5302:d200::1#53(2600:9000:5302:d200::1) for
detect-remediate.cloud.malwarebytes.com failed: network unreachable.
cloud.malwarebytes.com. 86400   IN      NS      ns-1289.awsdns-33.org.
cloud.malwarebytes.com. 86400   IN      NS      ns-2046.awsdns-63.co.uk.
cloud.malwarebytes.com. 86400   IN      NS      ns-440.awsdns-55.com.
cloud.malwarebytes.com. 86400   IN      NS      ns-902.awsdns-48.net.
cloud.malwarebytes.com. 86400   IN      NSEC    cloud\000.malwarebytes.com.
NS RRSIG NSEC
cloud.malwarebytes.com. 86400   IN      RRSIG   NSEC 13 3 86400
20251114233340 20251113213340 43999 malwarebytes.com.
INbe/MhFZB8P4NCVyTXPQJqLFu3OEEE4CDDzUzIRgyqhiK9Tmw1Md2cs
eCdhmtwUSXFCEcGb12AvNKabavbW0A==
;; Received 362 bytes from 205.251.199.253#53(ns-2045.awsdns-63.co.uk) in
17 ms

detect-remediate.cloud.malwarebytes.com. 60 IN A 18.210.92.144
detect-remediate.cloud.malwarebytes.com. 60 IN A 98.89.234.153
detect-remediate.cloud.malwarebytes.com. 60 IN A 98.88.154.173
detect-remediate.cloud.malwarebytes.com. 60 IN A 54.144.203.126
cloud.malwarebytes.com. 172800  IN      NS      ns-1289.awsdns-33.org.
cloud.malwarebytes.com. 172800  IN      NS      ns-2046.awsdns-63.co.uk.
cloud.malwarebytes.com. 172800  IN      NS      ns-440.awsdns-55.com.
cloud.malwarebytes.com. 172800  IN      NS      ns-902.awsdns-48.net.
;; Received 269 bytes from 205.251.193.184#53(ns-440.awsdns-55.com) in 6 ms
```

b. Root server: 199.7.91.13#53(d.root-servers.net)
c. TLD: 192.33.14.30#53(b.gtld-servers.net)
d. Yes, ns-2045.awsdns-63.co.uk
e. 5,9,17,6 ms

4. Output Analysis
    a. Determine what percentage of DNS queries did not return a response for each resolver.
        i. Do the two resolvers differ in this regard?
            1. No, each had 138 websites that didn't respond
        ii. If so, for which sites did the resolvers respond differently?
    b. Determine the average number of addresses returned per site for each resolver, as well as the standard deviations.
        i. Do the two resolvers differ in this regard?
            1. Yes
        ii. If so, by how much and in what ways?
            1. On average, Carleton receives more ip addresses per website (μ = 4.754820937) while the amount of addresses from a website

received are less clustered (σ = 5.56259684) compared to google’s μ = 4.749311295 and σ = 5.599967277.

c. For how many websites did you receive different IP address answers from the two resolvers?
    i. There were 218 websites that returned addresses that didn’t match from the resolvers
d. Compute the average TTL and standard deviation of the TTL for each of the 2 resolvers.
    i. Do the two resolvers differ in this regard?
        1. Yes
    ii. If so, by how much?

	TTL avg	TTL sd
carleton	1020.561983	4304.222863
google	795.4793388	2370.711991