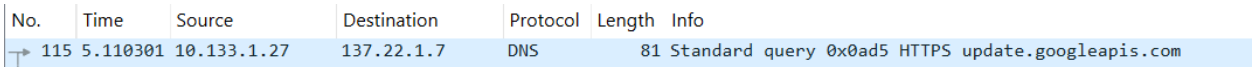
Part 1

Note: For the trace, I used the Raaid_full_trace.pcapng provided in the Artifacts folder.

Query: DNS Packet #115 from my trace.



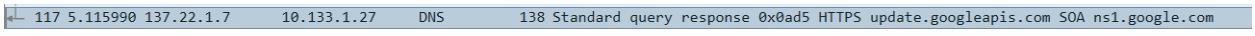
No.	Time	Source	Destination	Protocol	Length	Info
115	5.110301	10.133.1.27	137.22.1.7	DNS	81	Standard query 0x0ad5 HTTPS update.googleapis.com

3. DNS uses UDP since reliability is not important, and it just needs the response as fast as possible. If the message is lost, it can simply be retransmitted.

4.

- 1 Question
- Type: Standard Query
- Flag: Recursion desired
- Data:
    - Name: update.googleapis.com
    - [Name Length: 21]
    - [Label Count: 3]
    - Type: HTTPS (65) (HTTPS Specific Service Endpoints)
    - Class: IN (0x0001)

Response: DNS packet #117 from my trace.



117	5.115990	137.22.1.7	10.133.1.27	DNS	138	Standard query response 0x0ad5 HTTPS update.googleapis.com SOA ns1.google.com

5.

- 1 Response (packet #117)
- Name: googleapis.com, type: SOA, Class: IN, value: googleapis.com
- Response: message is a response, recursion is desired, recursion available

Part 2

1. Output

a. Windows IP Configuration

Host Name . . . . . : Raaid
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No

```
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : carleton.edu

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : A0-29-42-69-0E-93
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : A2-29-42-69-0E-92
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : carleton.edu
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   Physical Address. . . . . . . . . : A0-29-42-69-0E-92
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.133.1.27(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.224.0
   Lease Obtained. . . . . . . . . . : Monday, November 10, 2025 11:05:32 AM
   Lease Expires . . . . . . . . . . : Monday, November 10, 2025 4:33:13 PM
   Default Gateway . . . . . . . . . : 10.133.0.254
   DHCP Server . . . . . . . . . . . : 137.22.94.2
   DNS Servers . . . . . . . . . . . : 137.22.1.7
                                       137.22.1.6
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : C8-7F-54-C9-CF-34
```

DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

b. Number of DNS servers: 2
c. Preferred: 137.22.1.7

2. Output

a.

```
; <<>> DiG 9.17.15 <<>> Youtube.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6475
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 75d918eb7467d6f0df96771c69123bf0215b69a730bdce67 (good)
;; QUESTION SECTION:
;Youtube.com.                IN      A

;; ANSWER SECTION:
youtube.com.          278     IN      A       172.217.4.46

;; AUTHORITY SECTION:
youtube.com.          78241   IN      NS      ns2.google.com.
youtube.com.          78241   IN      NS      ns3.google.com.
youtube.com.          78241   IN      NS      ns1.google.com.
youtube.com.          78241   IN      NS      ns4.google.com.

;; ADDITIONAL SECTION:
ns2.google.com.       83228   IN      A       216.239.34.10
ns1.google.com.       83228   IN      A       216.239.32.10
ns3.google.com.       83228   IN      A       216.239.36.10
ns4.google.com.       83228   IN      A       216.239.38.10
ns2.google.com.       80578   IN      AAAA    2001:4860:4802:34::a
ns1.google.com.       80578   IN      AAAA    2001:4860:4802:32::a
ns3.google.com.       80578   IN      AAAA    2001:4860:4802:36::a
ns4.google.com.       80578   IN      AAAA    2001:4860:4802:38::a

;; Query time: 8 msec
;; SERVER: 137.22.1.7#53(137.22.1.7) (UDP)
;; WHEN: Mon Nov 10 13:24:32 Central Standard Time 2025
;; MSG SIZE  rcvd: 347
```

b. **Query**:
   - 1 Question
   - Type of query: A (IPV-4)
   - name: Youtube.com, TTL: 278, Type: A, class: IN, value: 172.217.4.46/
   - flags: qr rd ra
   - Data: Name: Youtube.com, Type: A, Class: IN

   Response:
   - 1 Answer
   - name: Youtube.com, TTL: 278, Type: A, class: IN, value: 172.217.4.46/
   - flags: qr rd ra

c. Here, the response is a Type A record because I directly queried for the IP address, whereas earlier I saw an SOA record because the server was providing zone-authority information.

   The name server appears as Google in my Wireshark trace (my local resolver) but as YouTube/Google-owned authoritative servers in dig, since Google manages YouTube's DNS. Wireshark exposes full packet-level details that dig summarizes, while dig also shows the authoritative and additional sections that Wireshark does not format explicitly.

3. Output

```
; <<>> DiG 9.17.15 <<>> youtube.com +trace
;; global options: +cmd
.                       319114  IN      NS      e.root-servers.net.
.                       319114  IN      NS      h.root-servers.net.
.                       319114  IN      NS      f.root-servers.net.
.                       319114  IN      NS      m.root-servers.net.
.                       319114  IN      NS      d.root-servers.net.
.                       319114  IN      NS      k.root-servers.net.
.                       319114  IN      NS      l.root-servers.net.
.                       319114  IN      NS      i.root-servers.net.
.                       319114  IN      NS      j.root-servers.net.
.                       319114  IN      NS      g.root-servers.net.
.                       319114  IN      NS      c.root-servers.net.
.                       319114  IN      NS      b.root-servers.net.
.                       319114  IN      NS      a.root-servers.net.
.                       386931  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 137.22.1.7#53(137.22.1.7) in 4 ms

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 20251125170000
20251112160000 61809 .
L8Wg03lEHatNHy0s/qDMwaFdwpErSsSZ6SIq9nB7SMk2OUqpAWgMaJlu
XQbk15rnuh8M915pYq9jUzs8XmsRojWb299ys+1kEeYQ75WiD3K/mhfc
Z4J8KLaSpojUogqJM1yY0Lru5tLMNyxe5C0pscE7B0hvgNtjtwh0+8Sn
r2Bgf+nXggXo/A6cl7s+OT5gSetAoYcKoVbncvC+Z93jYU+Jm8fZtQgx
aHSDLVqm5/wQrEQbA2JGH7XMM9YXpNiHFqxxeeeizb/MNJq2wZI1ftgW
kra9O6s61mFs2EV3VF6n0G7K2t3aRM+ndM5KU218zyMQgBk/tfQ9g6RD 6bgeGQ==
;; Received 1171 bytes from 192.203.230.10#53(e.root-servers.net) in 8 ms

youtube.com. 172800 IN NS ns2.google.com.
youtube.com. 172800 IN NS ns1.google.com.
youtube.com. 172800 IN NS ns3.google.com.
youtube.com. 172800 IN NS ns4.google.com.
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 900 IN NSEC3 1 1 0 -
CK0Q3UDG8CEKKAE7RUKPGCT1DVSSH8LL NS SOA RRSIG DNSKEY
NSEC3PARAM
CK0POJMG874LJREF7EFN8430QVIT8BSM.com. 900 IN RRSIG NSEC3 13 2 900
20251119002640 20251111231640 46539 com.
sau3mG+oYBapwhm/FNYkHjba2EYBCC4xVnGUOsx/lAUJlgTkq6MIlP9w
6LcXD5Slk8ck1N0mesF+3ubljSQLdg==
H5AIV1BJHPEF1R6U8P4TD6BJRD9HIKDA.com. 900 IN NSEC3 1 1 0 -
H5AJ5DQDTCKM5F19LA4UB4HGPFK6F6S4 NS DS RRSIG
H5AIV1BJHPEF1R6U8P4TD6BJRD9HIKDA.com. 900 IN RRSIG NSEC3 13 2 900
20251119001842 20251111230842 46539 com.

fCpWd7+SztagrDiDqlPGhXU3Dox6H02RDoP8qI6FdGbKegSZDckiPWT0
krrnz8sps921hLvGDbzjjShhF2T04A==
;; Received 652 bytes from 192.42.93.30#53(g.gtld-servers.net) in 21 ms

youtube.com. 300 IN A 142.250.191.174
;; Received 56 bytes from 216.239.32.10#53(ns1.google.com) in 34 ms

A. e.root-servers.net
B. g TLD Google server (g.gtld-servers.net)
C. ns1.google.com
D.

- Local: 4ms
- Root: 8ms
- TLD: 21ms
- Authoritative: 34 ms

Part 4

1.

a. 1.272% of Carleton and 1.274% of Google queries did not return a response.
b. (Analyzed within spreadsheet).

2.

a. The average number of IPs for Carleton was 3.46 and 3.436 for Google. Carleton had a standard deviation of 5.236, and Google had a standard deviation of 5.185. This means Google had slightly less variability.

3.

a. 221 websites returned different results.

4.

a. The average TTLs for Carleton was 872.689, and the standard deviation was 4879.007. The average TTLs for Google was 751.599, and standard deviation was 2233.887. This means Google cached more frequently than Carleton.