Week 11: DNS + Transport Layer (UDP: User Datagram Protocol)

Question1: . Answer the following questions in context of the DNS response (a.k.a, Resource Record RR) below:

A. How many answers were returned? What does it mean if the answer section is empty?
B. What is the time-to-live in this RR in seconds?
C. How many additional records are present?

```
$ dig @a.root-servers.net www.freebsd.org +norecurse
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57494
;; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.freebsd.org.  IN  A

;; AUTHORITY SECTION:
org.  172800  IN  NS  b0.org.afilias-nst.org.
org.  172800  IN  NS  d0.org.afilias-nst.org.

;; ADDITIONAL SECTION:
b0.org.afilias-nst.org.  172800  IN  A  199.19.54.1
d0.org.afilias-nst.org.  172800  IN  A  199.19.57.1
```

Question 2: Answer the following questions in context of the DNS response (a.k.a, Resource Record RR) below:, The dig query is asking a (.org server at 199.19.54.1) for the IP address of www.freebsd.org. How many answers were returned?

A. What do the authoritative records and additional records tell us?

```
$ dig @199.19.54.1 www.freebsd.org +norecurse
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39912
;; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 0

;; QUESTION SECTION:
;www.freebsd.org.  IN  A

;; AUTHORITY SECTION:
freebsd.org.  86400  IN  NS  ns1.isc-sns.net.
freebsd.org.  86400  IN  NS  ns2.isc-sns.com.
freebsd.org.  86400  IN  NS  ns3.isc-sns.info.
```

Question 3: Answer the following questions in context of the DNS response (a.k.a, Resource Record RR) below:

A. Assuming this is the next DNS query we do, following the query in Q3; list the server being contacted here, and whether this is an authoritative name server, top-level domain or the root server.

```
$ dig @ns1.isc-sns.net www.freebsd.org +norecurse
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17037
;; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;www.freebsd.org.  IN  A

;; ANSWER SECTION:
www.freebsd.org.  3600  IN  A  69.147.83.33

;; AUTHORITY SECTION:
freebsd.org.  3600  IN  NS  ns2.isc-sns.com.
freebsd.org.  3600  IN  NS  ns1.isc-sns.net.
freebsd.org.  3600  IN  NS  ns3.isc-sns.info.

;; ADDITIONAL SECTION:
ns1.isc-sns.net.  3600  IN  A  72.52.71.1
ns2.isc-sns.com.  3600  IN  A  38.103.2.1
ns3.isc-sns.info.  3600  IN  A  63.243.194.1
```

Question 4: Caching DNS Responses: The TTL (Time-to-live) values for Resource Records in the DNS should be..(provide your reasons)

A. Short, to make sure that changes are accurately reflected
B. Long, to avoid re-queries of higher-level DNS servers
C. Some combination depending on certain parameters (explain which)
D. Some other reason.

Attacking DNS

Security risk #1: malicious DNS server

- So far from what we have seen it seems as though if *any* of the DNS servers queried are malicious, they can lie to us and fool us about the answer to our DNS query.
- What are the potential consequences?
- Consider the following legitimate DNS response for eecs.mit.edu followed by a poisoned response. What are the consequences to www.swarthmore.edu with the poisoned DNS response?

Legitimate Response:

```
; ; <<>> DiG 9.6.0-APPLE-P2 <<>> eecs.mit.edu a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19901
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;eecs.mit.edu.                  IN    A

;; ANSWER SECTION:
eecs.mit.edu.           21600  IN    A     18.62.1.6
;; AUTHORITY SECTION:
mit.edu.                11088  IN    NS    BITSY.mit.edu.
mit.edu.                11088  IN    NS    W20NS.mit.edu.
mit.edu.                11088  IN    NS    STRAWB.mit.edu.

;; ADDITIONAL SECTION:
STRAWB.mit.edu.         126738 IN    A     18.6.6.6
BITSY.mit.edu.          166408 IN    A     18.72.0.3
W20NS.mit.edu.          126738 IN    A     18.70.0.160
```

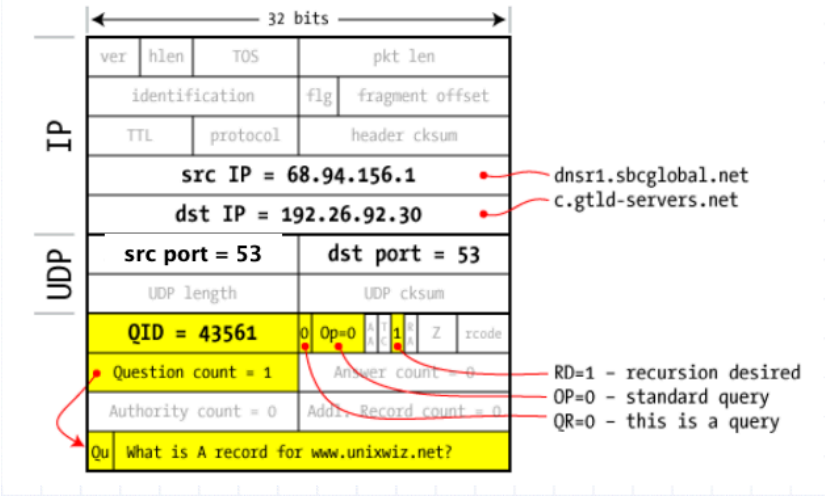
Poisoned DNS Response

```
; ; <<>> DiG 9.6.0-APPLE-P2 <<>> eecs.mit.edu a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19901
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;eecs.mit.edu.                  IN    A
;; ANSWER SECTION:
eecs.mit.edu.           21600  IN    A     18.62.1.6

;; AUTHORITY SECTION:
mit.edu.                11088  IN    NS    BITSY.mit.edu.
mit.edu.                11088  IN    NS    W20NS.mit.edu.
mit.edu.                30000  IN    NS    www.swarthmore.edu

;; ADDITIONAL SECTION:
www.swarthmore.edu.     30000  IN    A     18.6.6.6
BITSY.mit.edu.          166408 IN    A     18.72.0.3
W20NS.mit.edu.          126738 IN    A     18.70.0.160
```

Security risk #1: malicious DNS server: This form of attack is called a DNS cache poisoning attack. How could we go about preventing such an attack?

Security risk #2: on-path eavesdropper: If an attacker can eavesdrop on a DNS query from an unsuspecting client…. the client is toast.

- Use the following DNS query/response packet format to figure out what you can see as an on-path attacker that you can use to launch an attack.



Security risk #3: off-path attacker

• If an attacker can't eavesdrop on our traffic, can he inject spoofed DNS responses?

Mitigations to risks #2 and #3. What fields of the DNS header can you use to prevent man-in-the-middle and spoofing attacks?

DNSSEC offers authentication of known DNS servers using a chain-of-trust starting from the root server to an authoritative name server. How do you think the root server establishes its authenticity?

a. That's a single point of failure for DNSSEC
b. Another service establishes root server authenticity
c. A group of people ratify the root server authenticity
d. Some other way
e. Some combination of the above

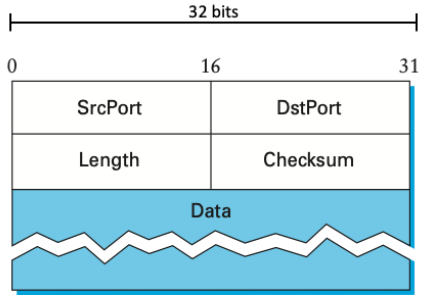
Q7. What kinds of attacks do you think are mitigated by using DNSSEC?

A. Amplification Attack
B. Cache Poisoning
C. Meddler-in-the-middle
D. DNS Redirection
E. DDoS (Distributed Denial of Service Attack)
F. DNS Injection

User Datagram Protocol (UDP) A.k.a best effort: ¯_(ツ)_/¯

UDP provides a datagram abstraction where:

A. The message is sent as a single packet
B. The application may break their data into datagrams each of which are received as a single unit on the receiving end.
C. There is no reliability or ordering guarantees.



Here is the UDP header: each field is of fixed length, followed by the payload which is a variable length field.
Q1. Why would we use UDP over TCP? (Hint: think of why DNS uses UDP)

A. UDP has less header state
B. UDP is faster
C. UDP is meaningless
D. You can custom build reliability at the application layer.

Q2. What kind of attacks can we launch with UDP?

A. Data injection
B. Data spoofing
C. Data reordering
D. Data replay attacks
E. DoS attacks

Q3. What guarantees does UDP provide?

A. Confidentiality
B. Availability
C. Integrity
D. Reliability
E. Ordering