Q1 *DNS over TCP (SU20 Final Q6)* (20 points)

Standard DNS uses UDP to send all queries and responses. Consider a modified DNS that instead uses TCP for all queries and responses.

Q1.1 (3 points) Which of the following does DNS over TCP guarantee against a man-in-the-middle attacker? Select all that apply.

☐ (A) Confidentiality   ☐ (C) Authenticity   ☐ (E) ——

☐ (B) Integrity   ☐ (D) None of the above   ☐ (F) ——

Q1.2 (3 points) Compared to standard DNS, does DNS over TCP defend against more attacks, fewer attacks, or the same amount of attacks against an on-path attacker?

○ (G) More attacks   ○ (I) Fewer attacks   ○ (K) ——

○ (H) Same amount of attacks   ○ (J) ——   ○ (L) ——

Q1.3 (5 points) What fields does an off-path attacker **not know** and need to **guess** correctly to spoof a response in DNS over TCP? Assume source port randomization is enabled. Select all that apply.

☐ (A) TCP sequence numbers   ☐ (C) Recursive resolver port   ☐ (E) DNS NS records

☐ (B) Name server port   ☐ (D) DNS A records   ☐ (F) None of the above

Q1.4 (3 points) Is the Kaminsky attack possible on DNS over TCP? Assume source port randomization is disabled.

○ (G) Yes, because the attacker only needs to guess the DNS Query ID

○ (H) Yes, but we consider it infeasible for modern attackers

○ (I) No, because the attacker cannot force the victim to generate a lot of DNS over TCP requests

○ (J) No, because TCP has integrity guarantees

○ (K) ——

○ (L) ——

Q1.5 (3 points) Recall the DoS amplification attack using standard DNS packets. An off-path attacker spoofs many DNS queries with the victim's IP, and the victim is overwhelmed with DNS responses.

Does this attack still work on DNS over TCP?

○ (A) Yes, the attack causes the victim to consume more bandwidth than the standard DNS attack

○ (B) Yes, the attack causes the victim to consume less bandwidth than the standard DNS attack

○ (C) No, because the DNS responses no longer provide enough amplification

○ (D) No, because the attacker cannot force the server to send DNS responses to the victim

○ (E) ——

○ (F) ——

Q1.6 (3 points) What type of off-path DoS attack from lecture is DNS over TCP vulnerable to, but standard DNS not vulnerable to? Answer in five words or fewer.

```



```

Q2   *Caltopia DNS (SP21 Final Q8)*   **(21 points)**

EvanBot is trying to determine the IP address of `caltopia.com` with DNS. However, some attackers on the network want to provide EvanBot with the wrong answer.
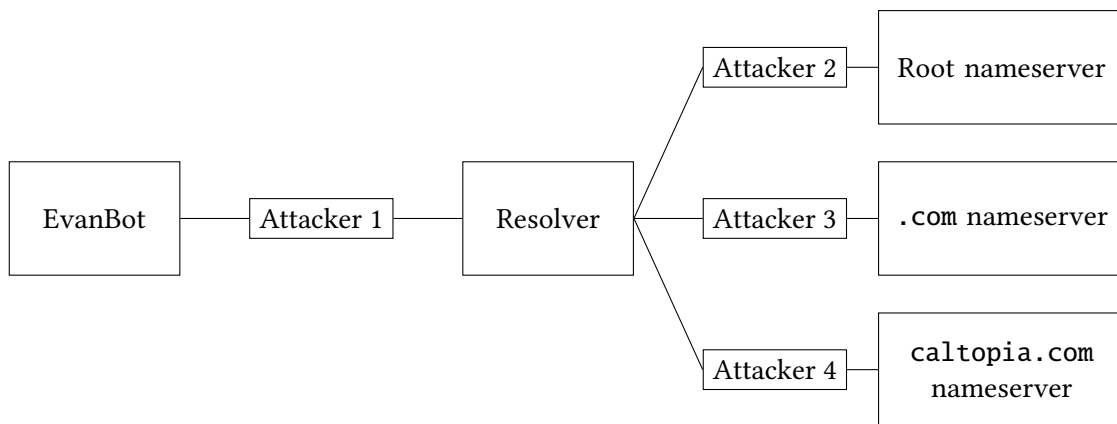
Assumptions:

- Each attacker is a man-in-the-middle (MITM) attacker between their two neighbors on the diagram above.

- No attackers can perform a Kaminsky attack.

- Standard DNS (not DNSSEC) is used unless otherwise stated.

- No private keys have been compromised unless otherwise stated.

- In each subpart, both EvanBot's cache and the local resolver's cache start empty.

- Each subpart is independent.

Clarification during exam: Assume that bailiwick checking is in use for this entire question.

In each subpart, EvanBot performs a DNS query for the address of `caltopia.com`.

Q2.1 (4 points) In this subpart only, assume the attackers only passively observe messages.

Which of the attackers would observe an `A` record with the IP address of `caltopia.com` as a result of EvanBot's query? Select all that apply.

☐ (A) Attacker 1   ☐ (C) Attacker 3   ☐ (E) None of the above

☐ (B) Attacker 2   ☐ (D) Attacker 4   ☐ (F) —

Q2.2 (3 points) Which of the attackers can poison the local resolver's cached record for `cs161.org` by injecting a record into the additional section of the DNS response? Select all that apply.

Note: Attacker 1 has intentionally been left out as an answer choice.

☐ (G) Attacker 2   ☐ (I) Attacker 4   ☐ (K) —

☐ (H) Attacker 3   ☐ (J) None of the above   ☐ (L) —

Q2.3 (4 points) Assume that the resolver and the name servers all validate DNSSEC, but EvanBot does not validate DNSSEC. Which of the attackers can poison EvanBot's cached record for `caltopia.com` by modifying the DNS response? Select all that apply.

☐ (A) Attacker 1   ☐ (C) Attacker 3   ☐ (E) None of the above

☐ (B) Attacker 2   ☐ (D) Attacker 4   ☐ (F) ——

Q2.4 (5 points) In this subpart only, assume the attackers only passively observe messages.

Assume that everyone validates DNSSEC. Which of the following records would Attacker 3 observe as a result of EvanBot's query? Select all that apply.

☐ (G) `DS` record with hash of the `.com` name server's public KSK

☐ (H) `DS` record with hash of the `caltopia.com` name server's public KSK

☐ (I) `A` record with the IP address of `caltopia.com`

☐ (J) `A` record with the IP address of the `caltopia.com` name server

☐ (K) `DNSKEY` record with the `.com` name server's public KSK

☐ (L) None of the above

Q2.5 (3 points) Assume that everyone validates DNSSEC, and the `caltopia.com` name server's private KSK has been compromised (i.e. all attackers know the `caltopia.com` name server's private KSK). No other private keys have been compromised.

Can EvanBot trust that they received the correct IP address of `caltopia.com`?

◯ (A) Yes, because the ZSK that signs the `A` record has not been compromised

◯ (B) Yes, because the trust anchor (the root's KSK) has not been compromised

◯ (C) No, because the compromised KSK can be used to sign a malicious `A` record

◯ (D) No, because the compromised KSK can be used to sign a fake ZSK that is used to sign a malicious `A` record

◯ (E) ——

◯ (F) ——

Q2.6 (2 points) TRUE or FALSE: DNSSEC prevents Attacker 4 from learning the IP address of `caltopia.com`.

◯ (G) True   ◯ (H) False   ◯ (I) ——   ◯ (J) ——   ◯ (K) ——   ◯ (L) ——

Q3 *Peter Parker in CS161: Training Wheels Protocol* **(7 points)**

There is an off-path attacker trying to poison Peter's DNS cache. This attacker wishes to trick Peter's recursive resolver into caching their IP address as the address of `cs161.org`. Assume Peter does not use DNSSEC and that Bailiwick checking is implemented.

Q3.1 (2 points) Select all true statements:

☐ The attacker must send a DNS response before the real nameserver responds to poison the cache

☐ The attacker must break symmetric key encryption to poison the cache

☐ The attacker must break asymmetric key encryption to poison the cache

☐ The attacker would not be able to poison the recursive resolver's cache if Peter's recursive resolver and all nameservers used DNSSEC

☐ None of the above

Q3.2 ($2\frac{1}{2}$ points) Which of the following domains, when visited by Peter using his browser, would give the attacker a non-negligible chance to poison the cache for `cs161.org`? Select all that apply.

☐ `https://cs161.org`

☐ `http://cs161.org`

☐ `http://nonexistentdomain.cs161.org`

☐ `http://www.google.com`

☐ `http://nonexistentdomain.google.com`

☐ None of the above

Q3.3 (2½ points) Now assume that Peter is a frequent visitor of `cs161.org` and `google.com` and that his recursive resolver has already cached those two domains. Which of the domains below may still give the attacker a non-negligible chance to poison the cache when Peter visits that domain? Select all that apply.

☐ `https://cs161.org`

☐ `http://cs161.org`

☐ `http://nonexistentdomain.cs161.org`

☐ `http://www.google.com`

☐ `http://nonexistentdomain.google.com`

☐ None of the above