1. (15 points) Bob wants to launch a Kaminsky DNS cache poisoning attack on a recursive DNS resolver; his goal is to get the resolver to cache a false IP address for the hostname www.example.com. Bob knows that during the iterative process, a query will be sent to the root server, then to the .com nameserver, and finally to the example.com nameserver. He can choose to spoof replies from any of these nameservers, after triggering the iterative process from the resolver. He decides to spoof a reply from the .com server. Please describe whether Bob's attack will be successful or not.

Spoofing an A record from the .com nameserver will not succeed against a resolver because .com is not authoritative for www.example.com. If Bob forges a fake delegation that the resolver accepts, he could then redirect www.example.com.

2. (15 points) A local DNS server decides to enforce the following policy: for any cached type NS record that has not expired, it can only be updated once every 20 minutes. For example, if the NS record for the example.com domain was created at time T, it cannot be updated until T plus 20 minutes or until the record expires, whichever comes earlier. Would this cause trouble for the Kaminsky attack? Please explain.

The 20-minute update-lock makes cache poisoning far harder by slowing replacement of NS delegations, but it doesn't prevent an attacker from succeeding on the initial attack or after TTL expiry.