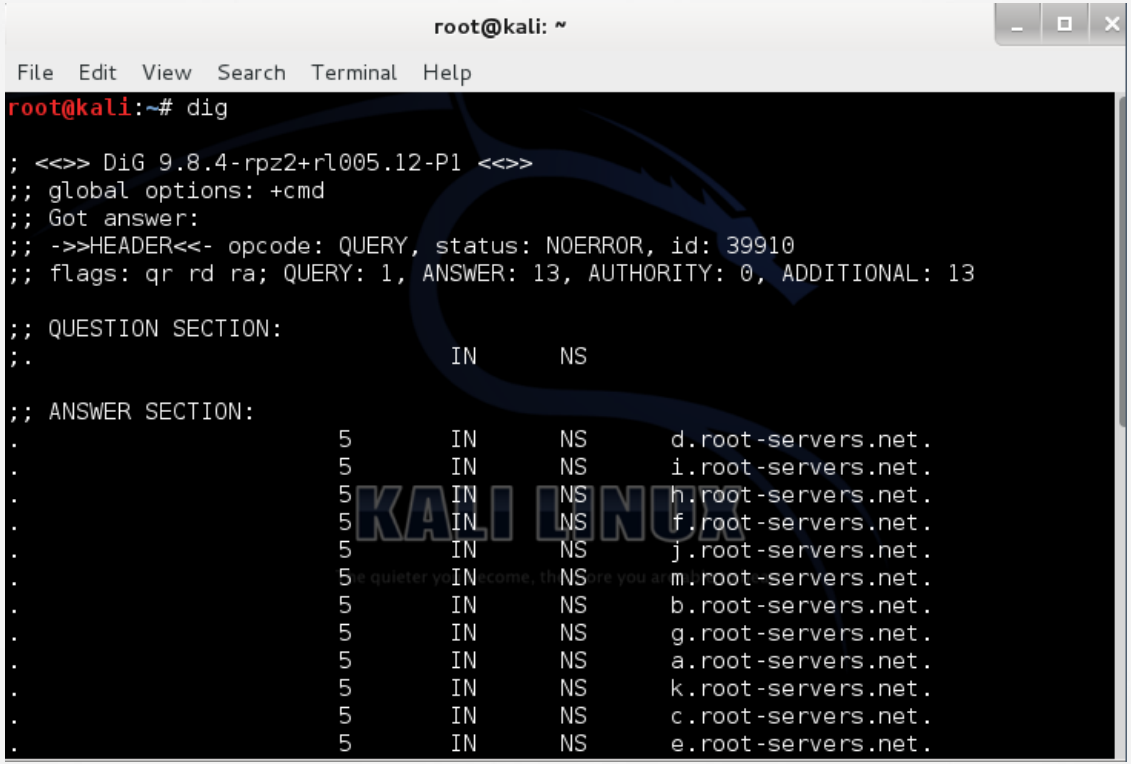
# Capturing DNS

# Capturing DNS

- What is DNS?
- Capturing DNS with Wireshark
  - You can filter via IP addresses
  - You can filter by port (53)
  - You can review the UDP stream

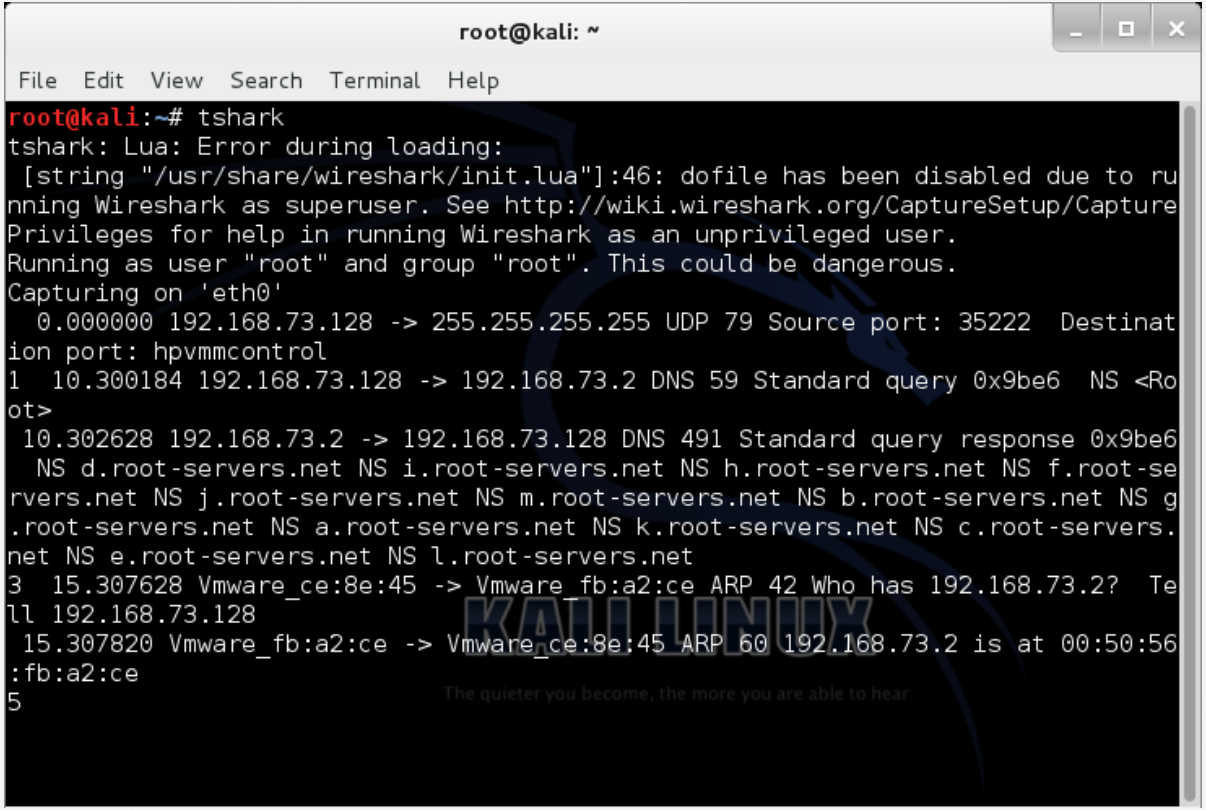
# Capturing DNS



# Capturing DNS

- **Using tshark**
  - You can run tshark from the command line. By running a simple dig, accessing a website, or attempting to access a resource by DNS name, you will capture DNS-related data.
- **Possible issues**
  - Poisoned DNS server
  - Failed DNS server
  - Stale records

# Capturing DNS



# Questions?