Lösung Wireshark Übung: DNS

1. Verwenden Sie "nslookup" um eine IP Adresse eines Web-Servers in den USA zu ermitteln. Wie lautet die IP Adresse des Web-Servers?

   ```
   $ nslookup www.mit.edu
   Server: 172.20.10.1
   Address: 172.20.10.1#53
   Non-authoritative answer:
   www.mit.edu
   canonical name = www.mit.edu.edgekey.net.
   www.mit.edu.edgekey.net
   canonical name = e9566.dscb.akamaiedge.net.
   Name: e9566.dscb.akamaiedge.net
   Address: 23.196.249.232
   ```

   Bei dem verwendeten Web-Server handelt es sich um den Webserver des Massachusetts Institute of Technology (MIT) in den USA. Die IP Adresse ist: 23.196.249.232

2. Verwenden Sie "nslookup" um die autoritativen Name Server einer Universität in Europa zu ermitteln.

   Um die autoritativen Name Server zu ermitteln muss der *Domain Resource Record Type „NS"* ermittelt werden.

   ```
   $ nslookup -type=NS kit.edu
   Server: 172.20.10.1
   Address: 172.20.10.1#53
   Non-authoritative answer:
   kit.edu nameserver = dns2.kit.edu.
   kit.edu nameserver = dns1.belwue.de.
   kit.edu nameserver = dns1.kit.edu.
   kit.edu nameserver = dns3.belwue.de.
   Authoritative answers can be found from:
   ```

   Die autoritativen Name Server für das Karlsruher Institute of Technology (KIT) sind: *dns*2.*kit.edu*, *dns*1.*belwue.de*, *dns*1.*kit.edu* und *dns*3.*belwue.de*. Die Antwort wurde von einem nicht-autoritativen Name Server mit der IP Adresse 172.20.10.1 erstellt.

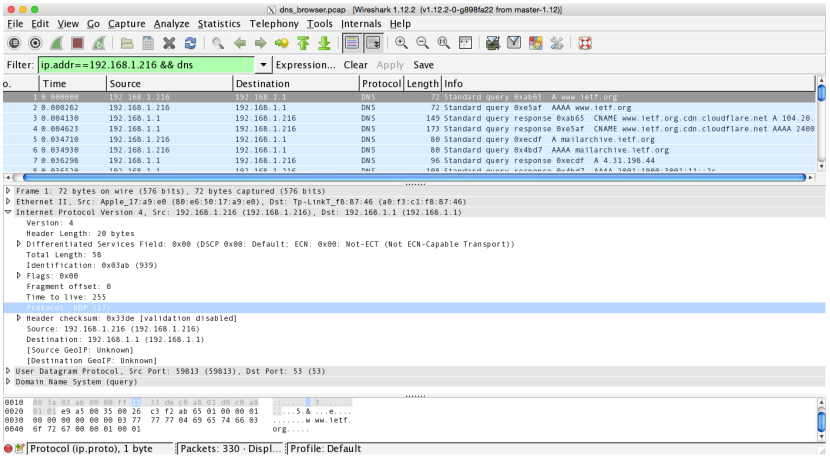
3. Ermitteln Sie die zuständigen Mail-Server der Universität (aus 2.) unter der Verwendung eines autoritativen Name Servers aus 2.

```
$ nslookup -type=MX kit.edu dns2.kit.edu
Server: dns2.kit.edu
Address: 129.13.65.10#53
kit.edu
mail exchanger = 10 scc-mailin-cn-01.scc.kit.edu.
kit.edu
mail exchanger = 100 scc-spamtrap-always-defer.scc.kit.edu.
kit.edu
mail exchanger = 10 scc-mailin-cs-01.scc.kit.edu.
kit.edu
mail exchanger = 5 scc-spamtrap-no-smtp-here.scc.kit.edu.
```

   Der oben angegebene Befehl ermittelt aller für die Domain *kit.edu* zuständigen Mail-Server unter Verwendung des autoritativen Domain Servers *dns*2.*kit.edu* welcher, unter anderen, im Aufgaben Teil 2. ermittelt wurde.

4. Finden Sie die "DNS Query" und "DNSResponse" Nachrichten. Welches Transportprotokoll wurde verwendet?

   Wie im *Protocol* Feld (IP Header) zu erkennen wurde UDP als Transportprotokoll verwendet.



5. Welche “Destination Port” wurde bei den “DNS Query” Nachrichten verwendet und welcher “Source Port” bei den “DNS Response” Nachrichten?

   Es wurde der „Destination Port“ 53 bei den „DNS Query“ Nachrichten verwendet, dies ist der Standard DNS Port.

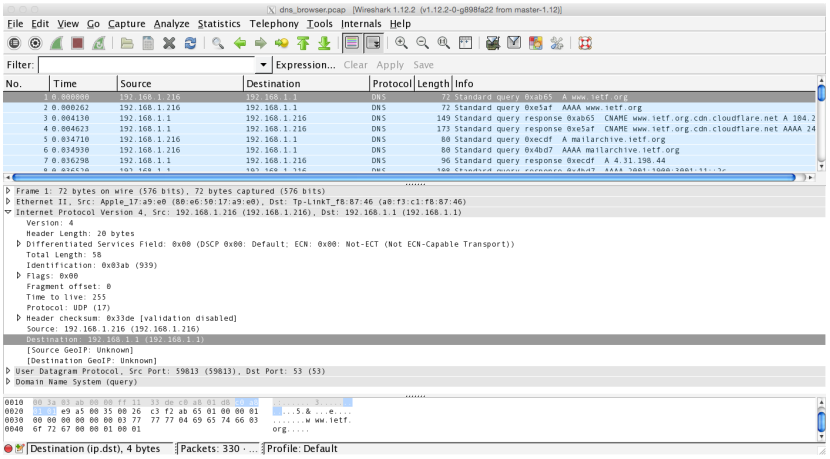
```
▷ Frame 1: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
▷ Ethernet II, Src: Apple_17:a9:e0 (80:e6:50:17:a9:e0), Dst: Tp-LinkT_f8:87:46 (a0:f3:c1:f8:87:46)
▷ Internet Protocol Version 4, Src: 192.168.1.216 (192.168.1.216), Dst: 192.168.1.1 (192.168.1.1)
▽ User Datagram Protocol, Src Port: 59813 (59813), Dst Port: 53 (53)
    Source Port: 59813 (59813)
    Destination Port: 53 (53)
    Length: 38
  ▷ Checksum: 0xc3f2 [validation disabled]
    [Stream index: 0]
▷ Domain Name System (query)
```

   Es wurde der „Source Port“ 53 bei den „DNS Response“ Nachrichten Verwendet, dies ist der Standard DNS Port.

```
▷ Frame 7: 96 bytes on wire (768 bits), 96 bytes captured (768 bits)
▷ Ethernet II, Src: Tp-LinkT_f8:87:46 (a0:f3:c1:f8:87:46), Dst: Apple_17:a9:e0 (80:e6:50:17:a9:e0)
▷ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.216 (192.168.1.216)
▽ User Datagram Protocol, Src Port: 53 (53), Dst Port: 54805 (54805)
    Source Port: 53 (53)
    Destination Port: 54805 (54805)
    Length: 62
  ▷ Checksum: 0xd4c2 [validation disabled]
    [Stream index: 2]
▷ Domain Name System (response)
```

6. Zu welcher IP-Adresse wurde die DNS Anfrage gesendet? Stimmt diese mit dem lokal konfigurierten überein?

   Die DNS Anfrage wurde an die IP Adresse 192.162.1.1 gesendet. Diese stimmt mit dem lokal konfigurierten DNS überein, dies lässt sich durch eine Überprüfung der lokalen Netzwerkeinstellungen feststellen.



7. Um was für eine "Query Type" handelt es sich? Welche Felder enthält die DNS Anfrage?

   Es handelt sich um eine Anfrage des Typs „A“. Die Anfrage enthält die Felder:

   - Name: Dieses enthält die angefragte Domain („$www.ietf.org$“)
   - Type: Dieses enthält den Anfrage Typ („A“)
   - Class: Dieses legt die Klasse des angefragten Records fest („IN“)

   Im wesentlichen handelt es sich bei den Feldern um die Daten eines „Ressource Domain Records“ (vergl. Vorlesungsunterlagen Applikationsschicht-DNS). Nicht angegeben sind „Time To Live“ und Value, diese werden in der Antwort erwartet!

```
▽ Domain Name System (query)
    [Response In: 3]
    Transaction ID: 0xab65
  ▷ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▽ Queries
    ▽ www.ietf.org: type A, class IN
        Name: www.ietf.org
        [Name Length: 12]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

8. Finden Sie die "DNS Response" Nachricht. Wie viele Antworten enthält diese und welche Felder sind jeweils enthalten?

   Die „DNS Response“ Nachricht ist, bei aktiven Display Filter („ip.addr==192.168.1.216 && dns“), nach der zweiten (IPv6 - Type: AAAA) DNS Anfrage zu finden. Sie enthält drei Antworten:

   (a) Eine von Typ „$CNAME$“, welche den Alias für ietf.org angibt.

   (b) Eine vom Typ „A“, welche die erste IP Adresse des Aliases angibt

   (c) Eine weitere vom Typ „A“, welche die zweite IP Adresse des Aliases angibt.

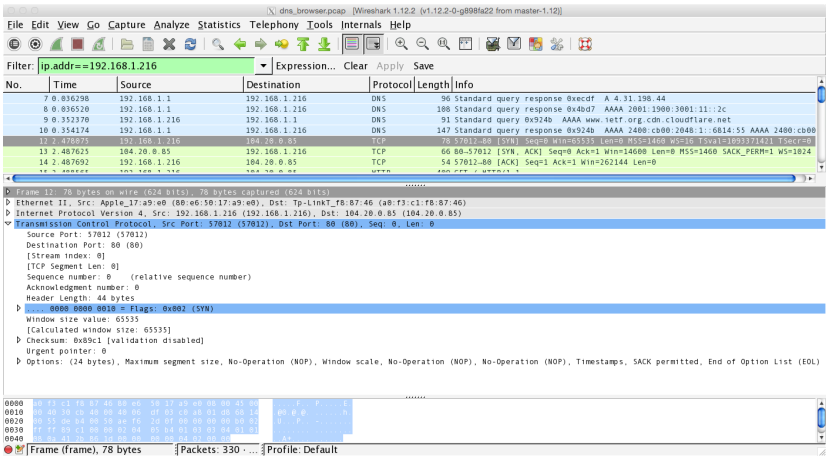
   Bemerkung: Bei einer Liste von IP Adressen wird der Client die Liste von oben (erster Eintrag) nach unten (Letzter Eintrag) abarbeiten.

Die Antworten enthalten jeweils den kompletten „Domain Resource Record“ (5-Tupel).

```
▽ Queries
  ▷ www.ietf.org: type A, class IN
▽ Answers
  ▷ www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
  ▽ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 222
      Data length: 4
      Address: 104.20.0.85 (104.20.0.85)
  ▽ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 222
      Data length: 4
      Address: 104.20.1.85 (104.20.1.85)
```

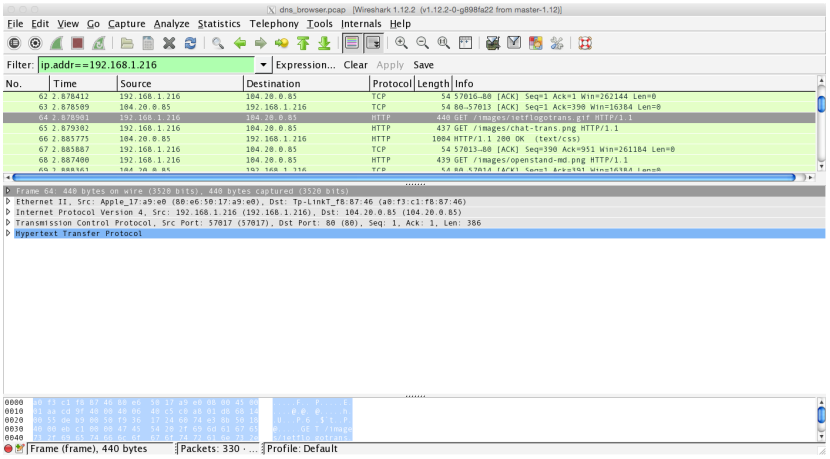
9. Entfernen Sie den “dns” Eintrag aus dem Display Filter und sehen Sie sich die SYN Pakete an, die Ihr Rechner gesendet hat. Stimmt die Zieladresse mit einer Adresse überein die Sie in einer “DNS Response” Nachricht finden können?

   Die SYN Pakete gehören zum Verbindungsaufbau (Handshake) der TCP Verbindung, welche zum Webserver (Port: 80) aufgebaut wird. Daher stimmt die Zieladresse mit der Adresse überein, die im DNS Response als erstes übermittelt wurde: 104.20.0.85



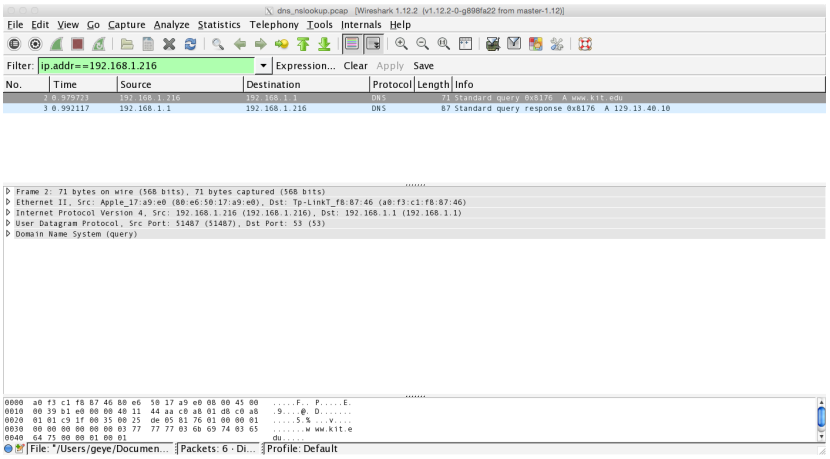
10. Die Webseite enthält Bilder. Wurden vom Browser weitere DNS Anfragen gestellt um diese Bilder nachzuladen?

    Nein, um Bilder unter einer bereits angefragten Domain nachzuladen werden keine weiter DNS Anfragen generiert. Die IP Adresse wird aus dem lokalen/Browser Cache bezogen.

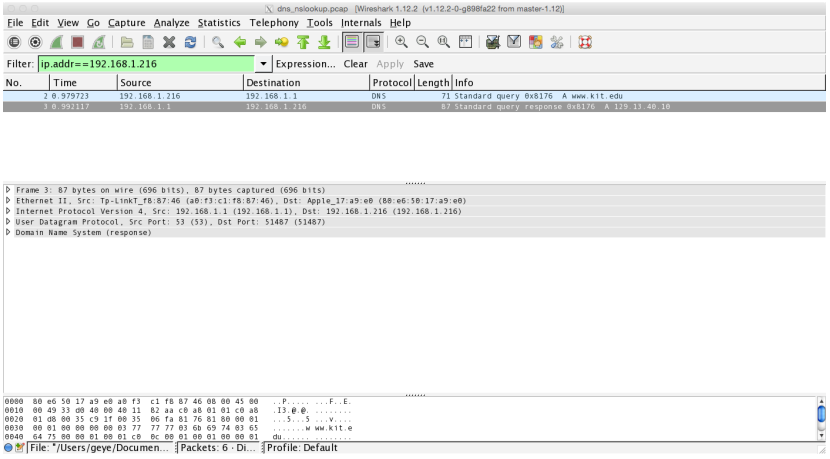


11. Welcher “Destination Port” wurde bei der “DNS Query” Nachricht verwendet und welcher “Source Port” bei der “DNSResponse” Nachricht?

    Beim „DNS Query“ wurde der „Destination Port: 53“ verwendet, der Standard DNS Port.



    Beim „DNS Response“ wurde der „Source Port: 53“ verwendet, der Standard DNS Port.



12. Zu welcher IP-Adresse wurde die DNS Anfrage gesendet? Stimmt diese mit dem lokal konfigurierten überein?

    Da beim „nslookup“ Befehl kein spezifischer DNS Server angegeben wurde, wurde der lokal konfigurierte DNS Server verwendet: 192.168.1.1 Dieser stimmt mit dem lokal konfigurierten überein.

13. Um was für einen “Query Type” handelt es sich? Welche Felder enthält die DNS Anfrage?

    Es handelt sich um eine Anfrage des Typs „A“. Die Anfrage enthält die Felder:

    - Name: Dieses enthält die angefragte Domain („$www.kit.edu$“)
    - Type: Dieses enthält den Anfrage Typ („A“)
    - Class: Dieses legt die Klasse des angefragten Records fest („IN“)

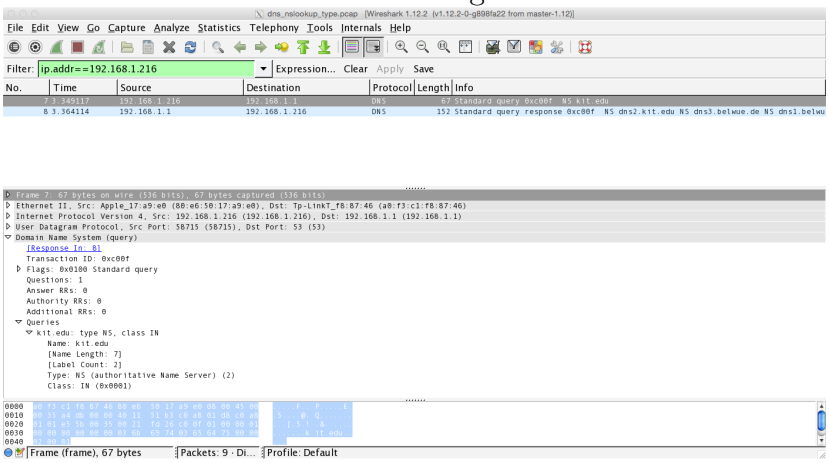
14. Wie viele Antworten enthält die “DNS Response” Nachricht und welche Felder sind jeweils enthalten?

    Die „DNS Response“ Nachricht enthält ein Antwort vom Typ „A“, welche die IP Adresse der nachgefragten IP enthält.

    Die Antworten enthält den kompletten „Domain Resource Record“ (5-Tupel).

15. Zu welcher IP-Adresse wurde die DNS Anfrage gesendet? Stimmt diese mit dem lokal konfigurierten überein?

    Da beim „nslookup“ Befehl kein spezifischer DNS Server angegeben wurde, wurde der lokal konfigurierte DNS Server verwendet: 192.168.1.1 Dieser stimmt mit dem lokal konfigurierten überein.



16. Um was für einen “Query Type” handelt es sich? Welche Felder enthält die DNS Anfrage?

    Es handelt sich um eine DNS Anfrage vom Typ „*NS*“. Die Anfrage enthält die Felder:

    - Name: Dieses enthält die angefragte Domain („*www.kit.edu*“)
    - Type: Dieses enthält den Anfrage Typ („*NS*“)
    - Class: Dieses legt die Klasse des angefragten Records fest („*IN*“)

```
Domain Name System (query)
    [Response In: 8]
    Transaction ID: 0xc00f
  ▷ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▽ Queries
    ▽ kit.edu: type NS, class IN
        Name: kit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
```

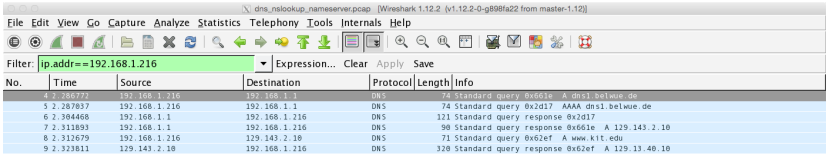
17. Wie viele Antworten enthält die “DNS Response” Nachricht? Sind auch IP Adressen der KIT Name Server enthalten?

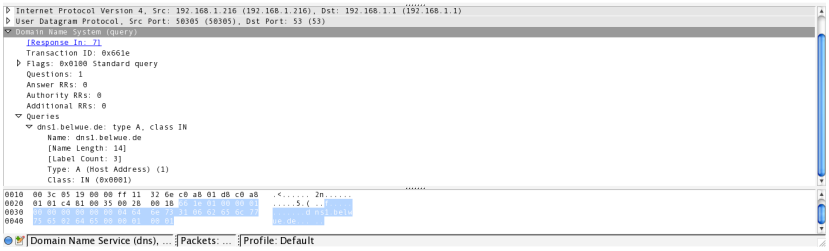
    Die „DNS Response“ enthält vier Antworten, diese enthalten die „” *NSType*“ Domain Resource Records und damit die Domain Namen der DNS Server nicht deren IP Adressen.

```
▽ Domain Name System (response)
    [Request In: 7]
    [Time: 0.014997000 seconds]
    Transaction ID: 0xc00f
  ▷ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
  ▷ Queries
  ▽ Answers
    ▷ kit.edu: type NS, class IN, ns dns2.kit.edu
    ▷ kit.edu: type NS, class IN, ns dns3.belwue.de
    ▷ kit.edu: type NS, class IN, ns dns1.belwue.de
    ▷ kit.edu: type NS, class IN, ns dns1.kit.edu
```

18. Wie viele “DNS Query” Nachrichten wurden insgesamt erzeugt? Zu welchen IP-Adressen wurden die DNS Anfragen gesendet? Mit welchen IP Adressen korrespondieren diese?

    Es wurden bei dieser Abfrage insgesamt zwei „DNS Query“ Nachrichten erzeugt (genau genommen drei wenn man die Type „*AAAA*“ mitrechnet - IPv6 IP des DNS!) Dies liegt daran, dass im ersten Schritt die IP Adresse des DNS ermittelt werden muss und in einem zweiten dann damit die IP der anzufragenden Domain.
    Die erste Anfrage (Auflösung DNS) wurde an den lokal konfigurieren DNS (192.168.1.1) geschickt, die zweite an die ermittelt IP des DNS *dns*1.*belwue.de* (129.143.2.10)





19. Wie viele Antworten enthalten die “DNS Response” Nachrichten?

    Die „DNS Response“ Nachricht enthält eine Type „A“ Antwort - die IP (129.13.40.10) der angefragen Domain ($www.kit.edu$), vier Type „NS“ Antworten mit den, für dei Domain zuständigen, autoritativen Name Servern sowie deren IPv4 und IPv6 Adressen (Type „A“ und Type „$AAAA$“