DHBW Karlsruhe
Duale Hochschule Baden-Württemberg

Netztechnik I

TINF

Wireshark

DNS

Markus Götzl
Dipl.-Inform. (FH)
mail@markusgoetzl.de

http://www.dhbw-karlsruhe.de

Wireshark

- Wireshark Ressourcen
- Mitschitt (Trace) erzeugen
- Trace Analyse

Wireshark Ressourcen

- Wireshark Homepage:
  - *http://www.wireshark.org*
- Wireshark Downloads:
  - http://www.wireshark.org/download.html
- Wireshark Dokumentation
  - *http://www.wireshark.org/docs/*

Trace erzeugen

Finden des Netzwerk-Interfaces und des Gateways

```
Themis:~ root# route -n get default
   route to: default
destination: default
       mask: default
    gateway: 192.168.2.1
  interface: en0
```

- Linux: `route`
- Windows: `route print`
- Mac: `route -n get default`

Trace erzeugen

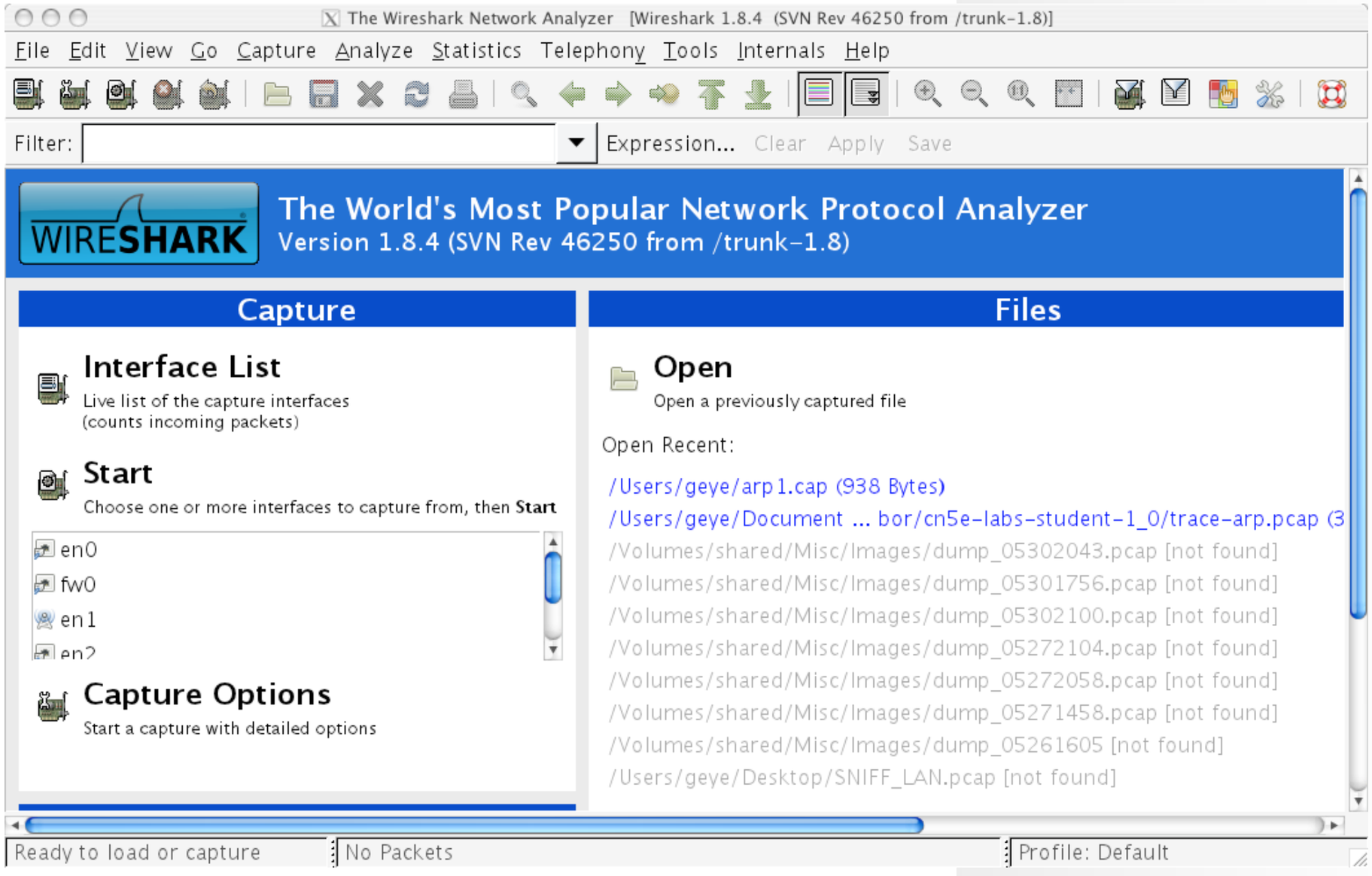
Finden der eigenen MAC-Adresse

```
themis:~ root# ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet6 fe80::223:32ff:feda:198c%en0 prefixlen 64 scopeid 0x4
        inet 192.168.2.107 netmask 0xffffff00 broadcast 192.168.2.255
        inet6 2003:6a:6f16:a601:223:32ff:feda:198c prefixlen 64 autoconf
        ether 00:23:32:da:19:8c
        media: autoselect (100baseTX <full-duplex,flow-control>) status: active
        supported media: none autoselect 10baseT/UTP <half-duplex> 10baseT/UTP <
full-duplex> 10baseT/UTP <full-duplex,flow-control> 10baseT/UTP <full-duplex,hw-
loopback> 100baseTX <half-duplex> 100baseTX <full-duplex> 100baseTX <full-duplex
,flow-control> 100baseTX <full-duplex,hw-loopback> 1000baseT <full-duplex> 1000b
aseT <full-duplex,flow-control> 1000baseT <full-duplex,hw-loopback>
```

- Linux: `ifconfig <device>`
- Windows: `ipconfig /all | more`
- Mac: `ifconfig <device>`

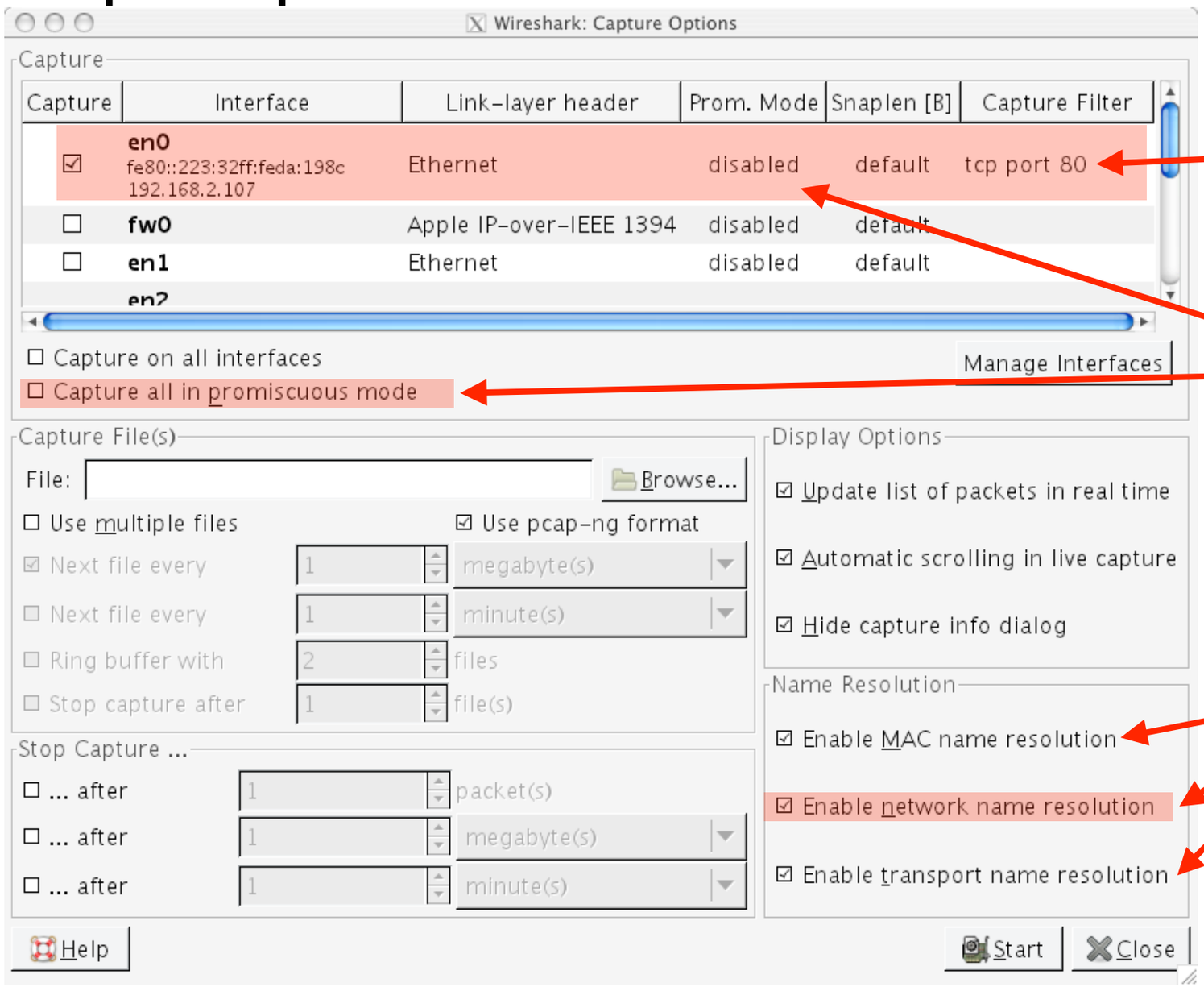
Trace erzeugen

Wireshark starten



Trace erzeugen

Capture Options



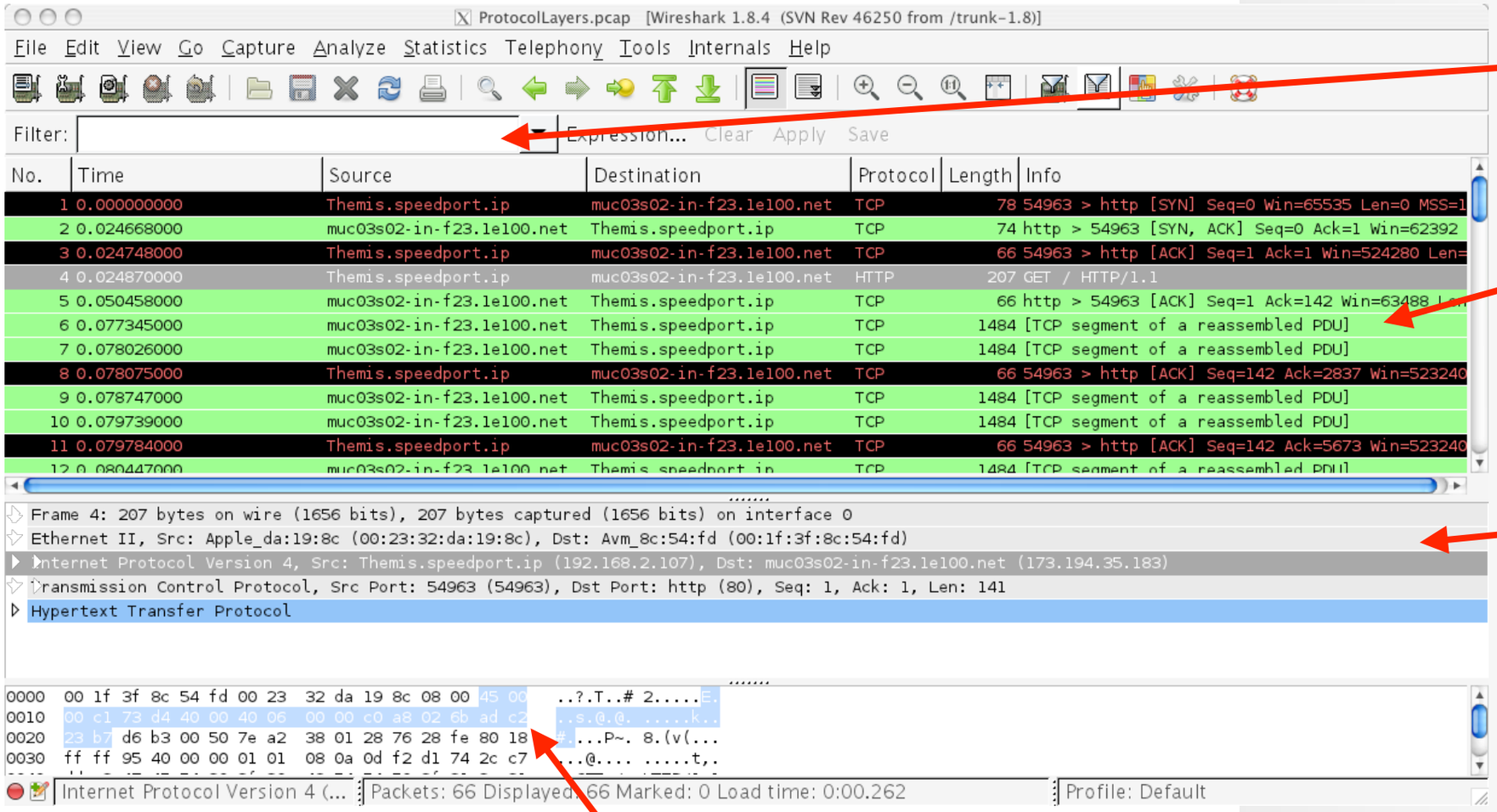
Capture Filter: "Vorfiltern" des Mitschnittes. Leer -> keine Filterung.

Nur Verkehr, der für dieses Gerät bestimmt ist.

Namensauflösung

Trace Analyse

Wireshark GUI



Display Filter

Darstellung der Mitschnitts nach Display Filter: Sortierung nach Zeitstempel, Quelle, Ziel, Protokoll, Länge und Kurzbeschreibung

Wireshark "Blocks": Protokollschichten Übersicht/Auswahl

Inhalt eines Rahmens HEX und ASCII

DNS

Vorbereitungen:

1. Für die Übung wird das Tool *“nslookup”* verwendet welches unter Unix/ Linux/Mac OS X und Windows zur Verfügung steht. Ein *“nslookup”* Kommando kann z.B. folgendermaßen formuliert werden:

   i. `nslookup www.kit.edu`
   Es wird die IP Adresse des Rechners www.kit.edu ermittelt.

   ii. `nslookup -type=NS mit.edu`
   Es es werden alle Namen der autoritativen Name Server für kit.edu ermittelt.

   iii. `nslookup www.nus.edu.sg resolver1.opendns.com`
   Es wird die IP Adresse von www.nus.edu.sg über den DNS resolver1.opendns.com ermittelt.

DNS

Vorbereitungen:

2. OS DNS Cache löschen:

   - Unter Windows kann ipconfig auch verwendet werden um den OS eigenen DNS cache zu verwalten:

     i. `ipconfig /displaydns`
     Gibt den aktuellen DNS Cache aus.

     ii. `ipconfig /flushdns`
     Löscht den DNS Cache

   - Unter Mac OS X (ab 10.6) kann der DNS Cache mit folgenden Befehl (beenden des Cache-Prozesses): `sudo killall -HUP mDNSResponder`

DNS

Vorbereitungen:

- Unter Linux wird meist kein DNS Catche verwendet. Falls *“nscd - Name Service Cache Daemon”* verwendet wird kann diese mit folgenden Befehl gelöscht werden:
  i. Alle User: `sudo nscd -I hosts`
  ii. Nur der aktuelle user: `sudo nscd -i hosts`

DNS

Fragen:

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

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

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

DNS

Fragen:

- Leeren Sie den OS DNS Cache sowie den Browser Cache. Starten Sie Wireshark und starten Sie einen Mitschnitt Danach verwenden Sie bitte Ihren Browser um die Webseite der IETF zu besuchen (`http://www.ietf.org`). Wenn die Seite vollständig aufgebaut ist beenden Sie bitte den Wireshark-Mitschnitt. Filtern Sie nach DNS Paketen welche Ihre eigene IP Adresse enthalten (`ip.addr==<eigene IP Adresse> && dns`)

4. Finden Sie die *“DNS Query”* und “DNS*Response”* Nachrichten. Welches Transportprotokoll wurde verwendet?

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

DNS

Fragen:

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

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

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

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?

DNS

Fragen:

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

- Starten Sie einen neuen Mitschnitt via Wireshark und rufen Sie über die Kommandozeile `nslookup www.kit.edu` auf. Danach beenden Sie bitte den Mitschnitt.

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

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

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

DNS

Fragen:

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

- Starten Sie einen neuen Mitschnitt via Wireshark und rufen Sie über die Kommandozeile `nslookup -type=NS www.kit.edu` auf. Danach beenden Sie bitte den Mitschnitt.

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

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

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

DNS

Fragen:

- Starten Sie einen neuen Mitschnitt via Wireshark und rufen Sie über die Kommandozeile `nslookup www.kit.edu dns1.belwue.de` auf. Danach beenden Sie bitte den Mitschnitt.

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

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