DHBW Duale Hochschule Baden-Württemberg Karlsruhe

Netztechnik I

TINF

Wireshark

ICMP

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

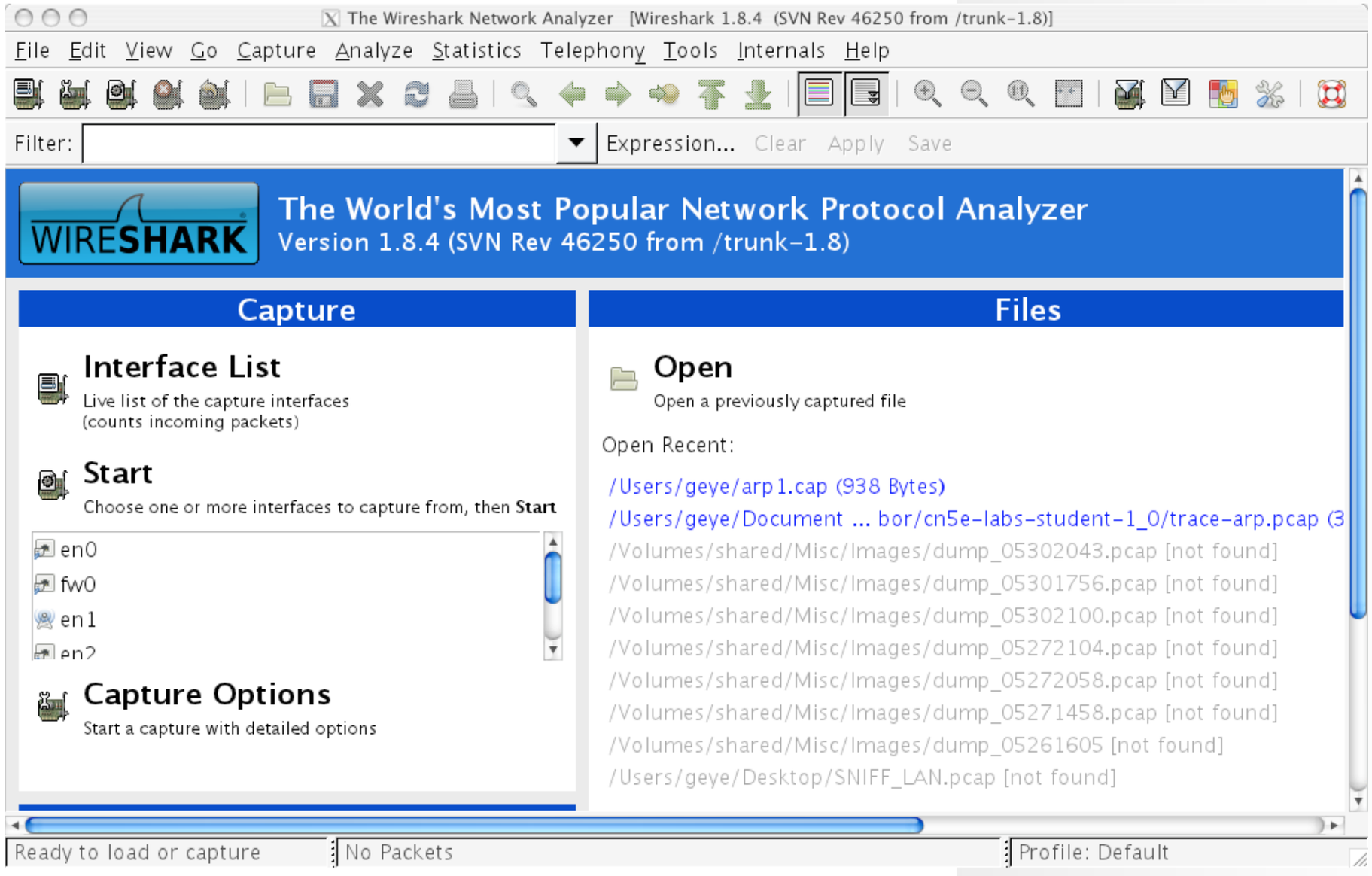
Finden der eigenen MAC-Adresse

```
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>`

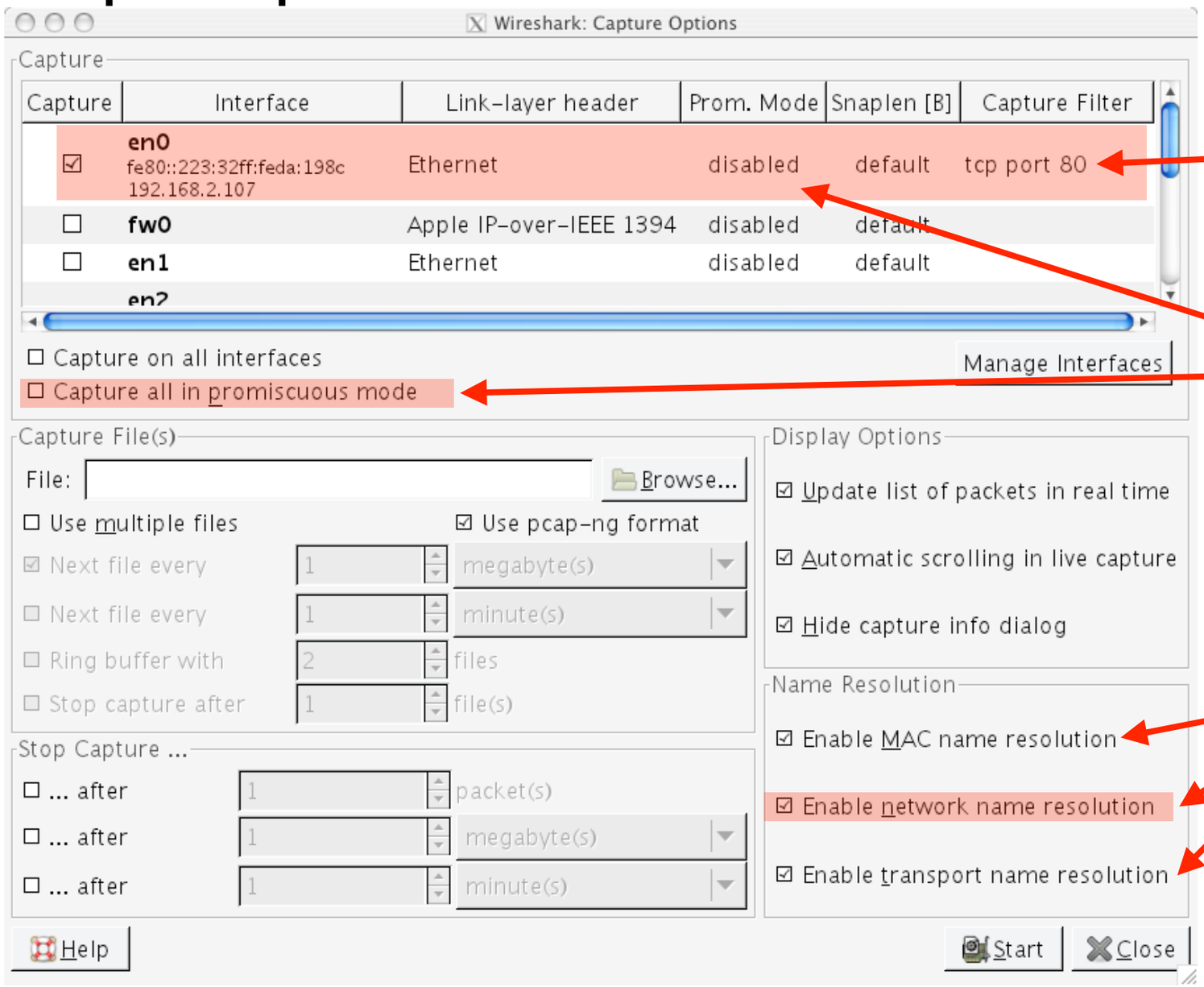
Trace erzeugen

Wireshark starten



Trace erzeugen

Capture Options



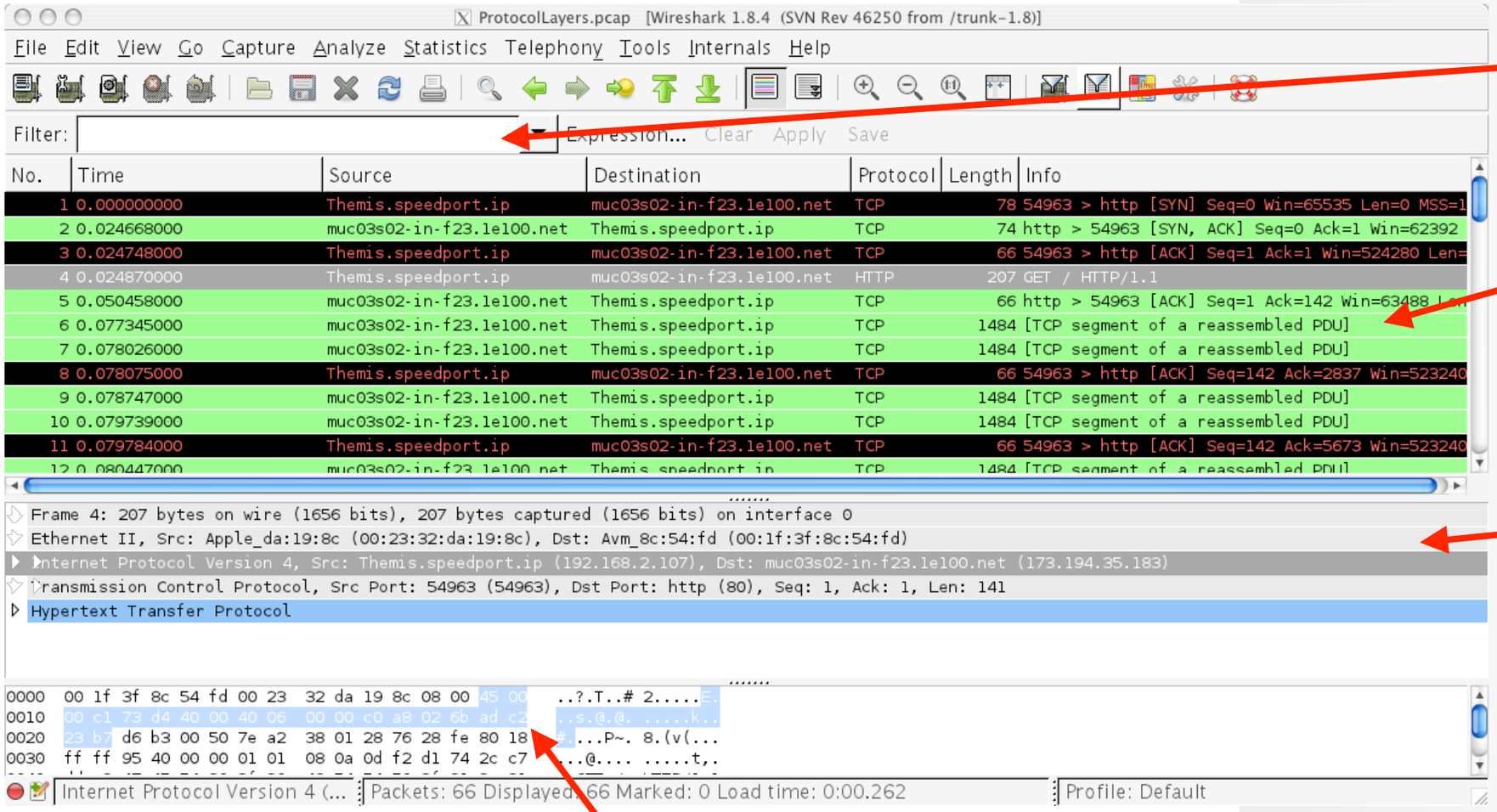
Capture Filter: "Vorfiltern" des Mitschnittes. Leer -> keine Filterung.

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

ICMP - Ping

Vorbereitungen:

1. Starten Sie einen Mitschnitt an dem Netzwerkinterface, welches aktuell an Ihrem Rechner für externe Verbindungen verwendet wird.

2. Starten Sie *“Ping”* mit einen Ziel außerhalb Europas z.B. www.nsa.gov oder www.mit.edu für 10 Aufrufe (Windows: `ping -n 10 <host>`, OS X / Linux: `ping -c <host>`)

3. Beenden Sie den Mitschnitt sobald die 10 *“Ping”* Aufrufe beendet sind (ping terminiert).

4. Filtern alle nicht ICMP Pakete mit Hilfe des Display Filters aus.

ICMP - Ping

Fragen:

1. Wie lautet die IP Adresse Ihres Rechners?
2. Wie lautet die IP Adresse des Ziel Rechners
3. Warum haben die *“ICMP Pakete”* kein Ziel-/Quell-Port (Portnummer)?
4. Wählen Sie ein ICMP Paket aus, welches von Ihrem Rechner versendet wurde. Welchen Wert haben die Felder *“Type”* und *“Code”* ? Welche Felder besitzt das ICMP Paket außerdem und wie groß (Bytes) sind diese?
5. Wählen Sie ein korrespondierendes *“Ping replay Paket”* aus. Welchen Wert haben die Felder *“Type”* und *“Code”* ? Welche Felder besitzt das ICMP Paket außerdem und wie groß (Bytes) sind diese?

ICMP - Traceroute

Vorbereitungen:

1. Starten Sie einen Mitschnitt an dem Netzwerkinterface, welches aktuell an Ihrem Rechner für externe Verbindungen verwendet wird.

2. Starten Sie “`traceroute -I <host>`” (Windows: “`tracert <host>`”) mit einen Ziel außerhalb Europas z.B. www.nsa.gov oder www.mit.edu.

3. Beenden Sie den Mitschnitt sobald *“traceroute”* beendet ist.

4. Filtern alle nicht ICMP Pakete mit Hilfe des Display Filters aus.

ICMP - Traceroute

Fragen:

1. Wie lautet die IP Adresse Ihres Rechners?
2. Wie lautet die IP Adresse des Ziel Rechners
3. Wie lautet die *“IP Protocol Number”* wie erklärt sich diese Nummer anhängig vom Betriebsystem?
4. Unterscheidet sich eines der vorliegenden *“ICMP Echo Packet”* von einem *“ICMP Query Paket”* aus dem ersten Teil der Übung?
5. Untersuchen Sie ein “ICMP-Error Packet”. Wie unterscheidet sich dieses von einem *“ICMP Echo Packet”*?

ICMP - Traceroute

Fragen:

6. Untersuchen Sie die drei letzten ICMP Pakete, die der Quellrechner empfangen hat. Wie unterscheiden sich diese und warum?

7. Befindet sich unter den “tracert” bzw. “traceroute” Ausgaben ein Verbindungen (links) welche eine signifikant längeren “Round Trip Delay” aufweisen? Wenn Ja, welche und warum?

ICMP - Challenge

- Gesucht ist eine Kommandozeile, welche alle Hosts (IP Adressen) liefert die sich im eigenen Netzwerk befinden und auf ICMP Echo Request antworten.

- Bitte nicht ausführen!