DHBW Duale Hochschule Baden-Württemberg Karlsruhe

Netztechnik I

TINF

Wireshark

IP Paket

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

http://www.dhbw-karlsruhe.de

Wireshark

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

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

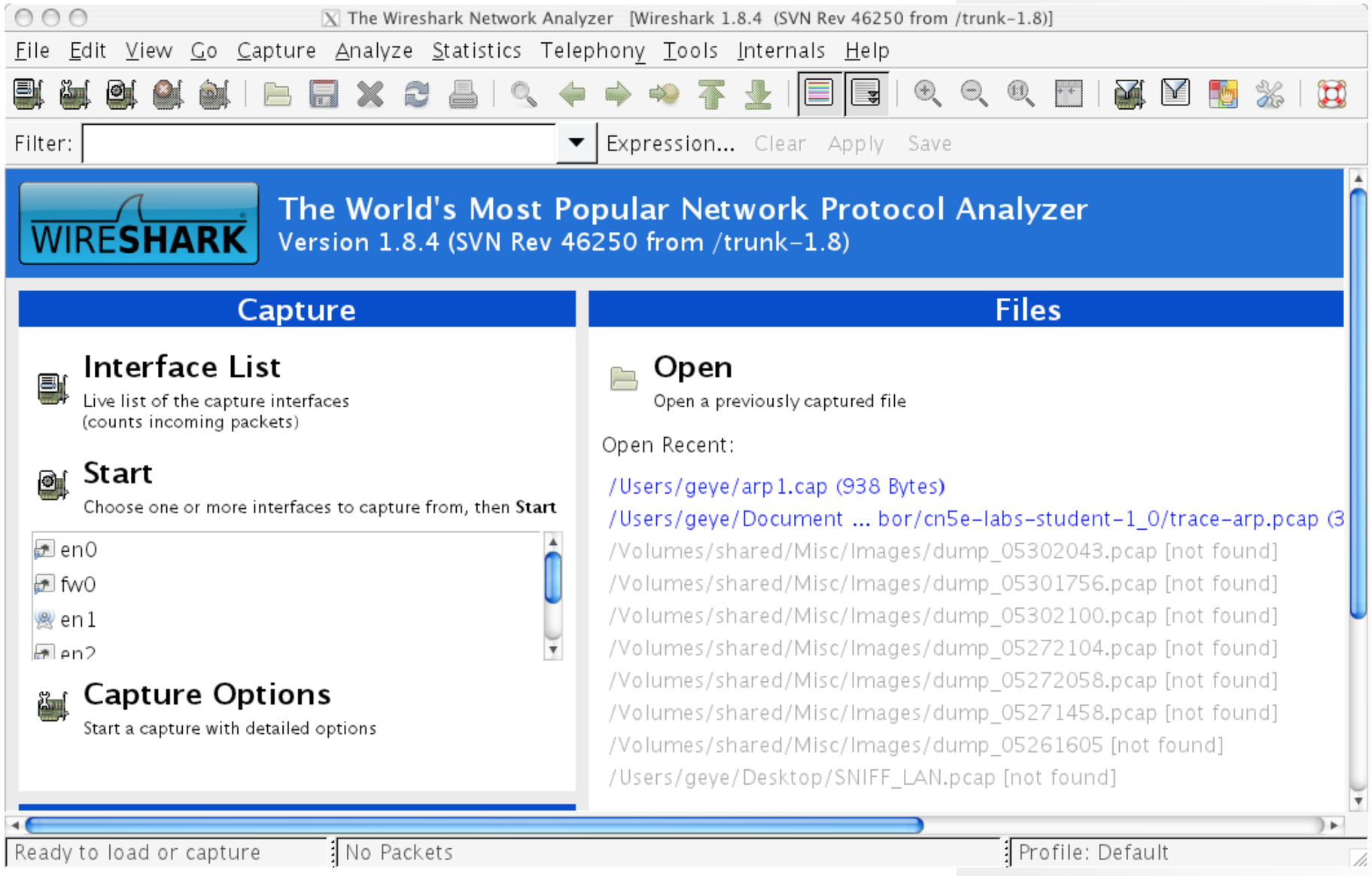
Finden des Netzwerk-Interfaces und des Gateways

```
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`

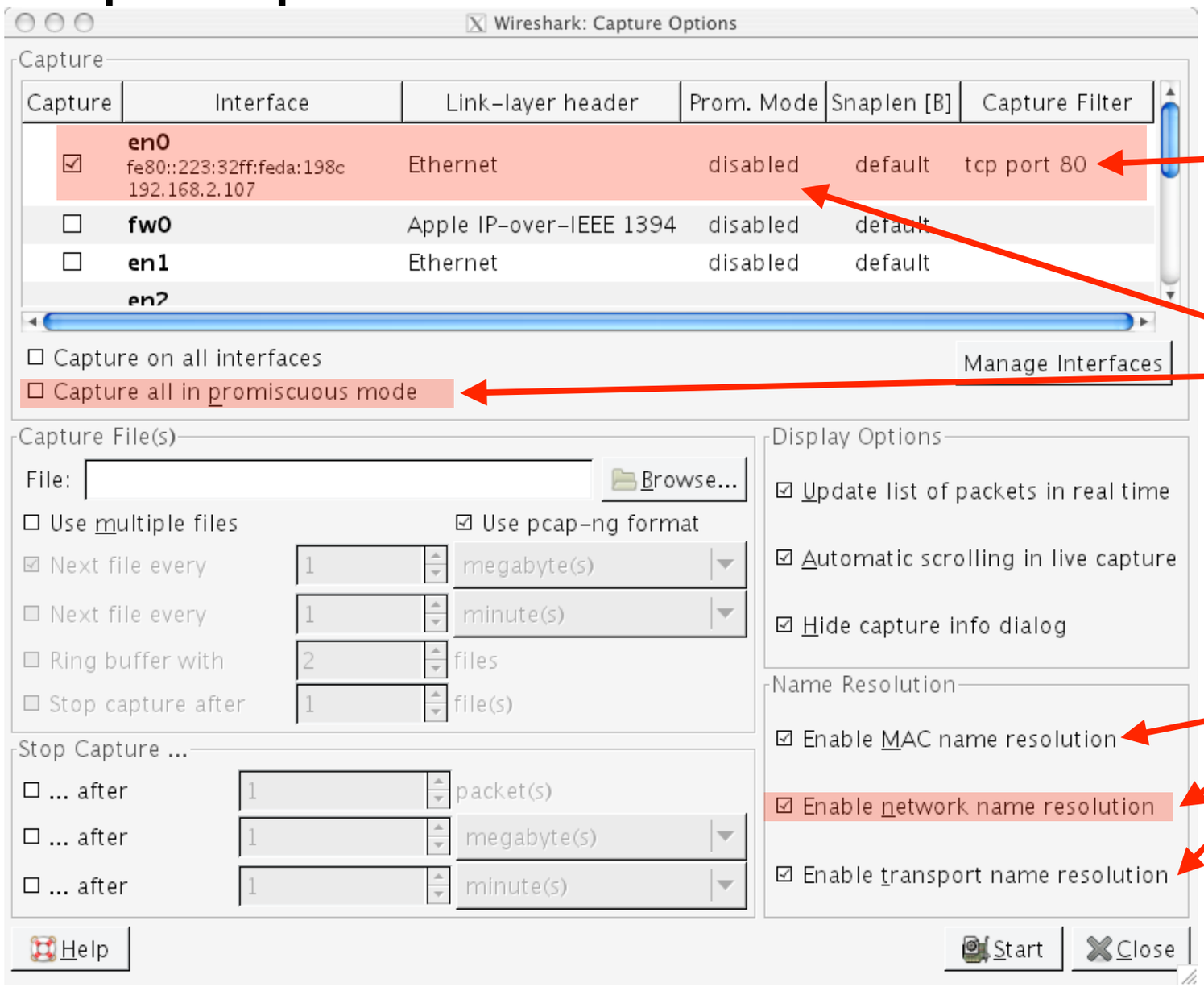
Trace erzeugen

Wireshark starten



Trace erzeugen

Capture Options



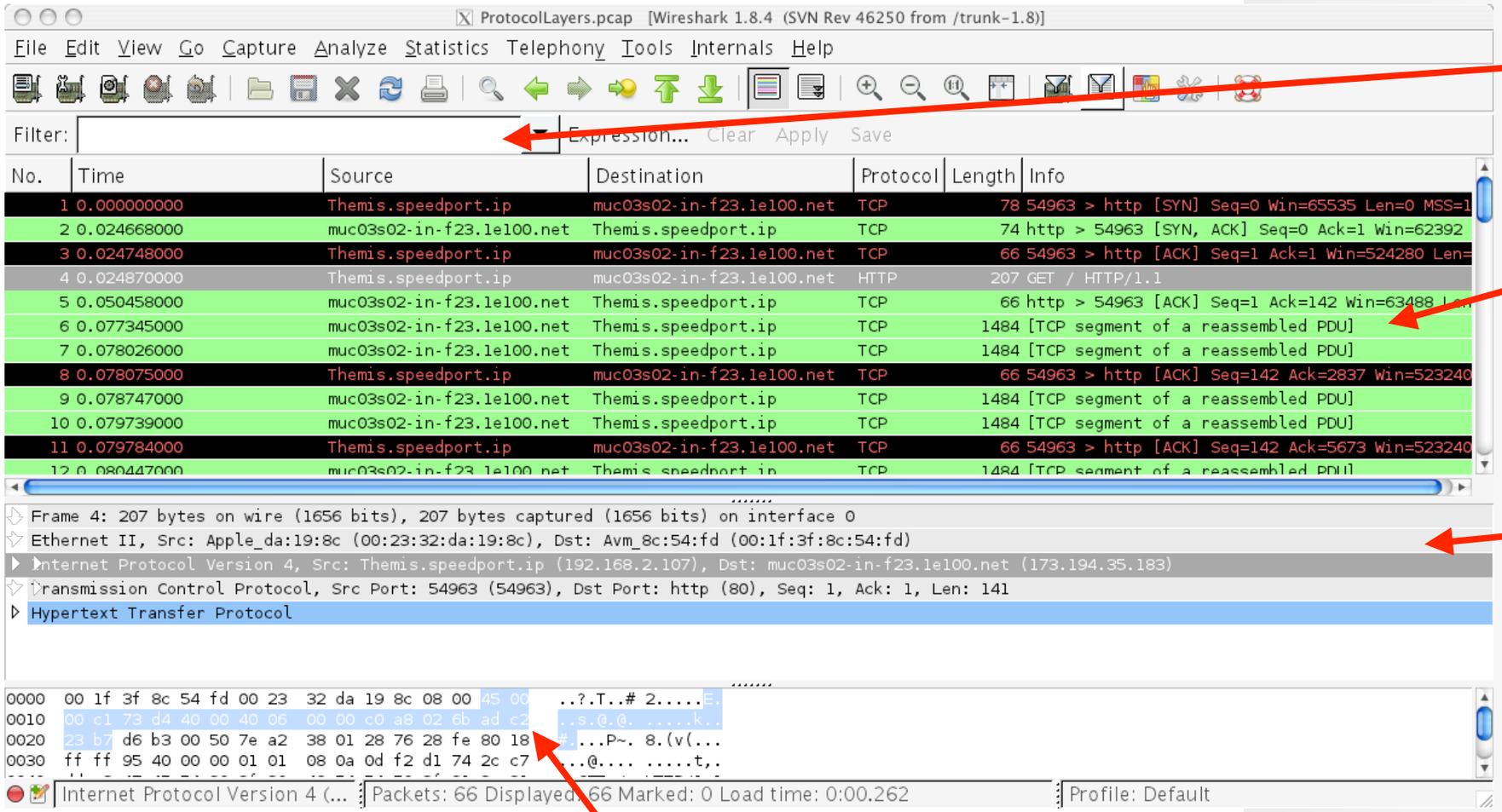
Capture Filter: "Vorfiltern" des Mitschnittes. Leer -> keine Filterung.

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

IP Paket

1. Öffnen Sie die Datei “`ip.pcap`” (Wireschark Capture File)

2. Wenden Sie einen *Display Filter* an um ausschließlich Frames anzeigen zu lassen, welche DNS Pakete (Domain Name Service) enthalten.

3. Wählen Sie einen Frame aus der von “Themis.local” (192.168.2.107) gesendet wurde und an den lokalen Router “speedport.ip” (192.168.2.1) adressiert ist.

   (a) Welche IP Version wurde verwendet?

   (b) Wie groß ist der IP Header und wie errechnet sich dieser Wert?

IP Paket

4. Für welches Feld werden die nächsten 8 bit verwendet und wie werden diese aufgeteilt?

5. Wie groß ist das IP Paket insgesamt?

6. Fragmentierung

   (a) Welche Identifikation hat das Paket und wurde es in mehrere Fragmente aufgeteilt?

   (b) Welchen Grund könnte es für eine Fragmentierung geben?

   (c) Welche Bedeutung hat das “DF” Flag?

7. Welches Schicht 4 (Transportschicht) Protokoll wird verwendet?