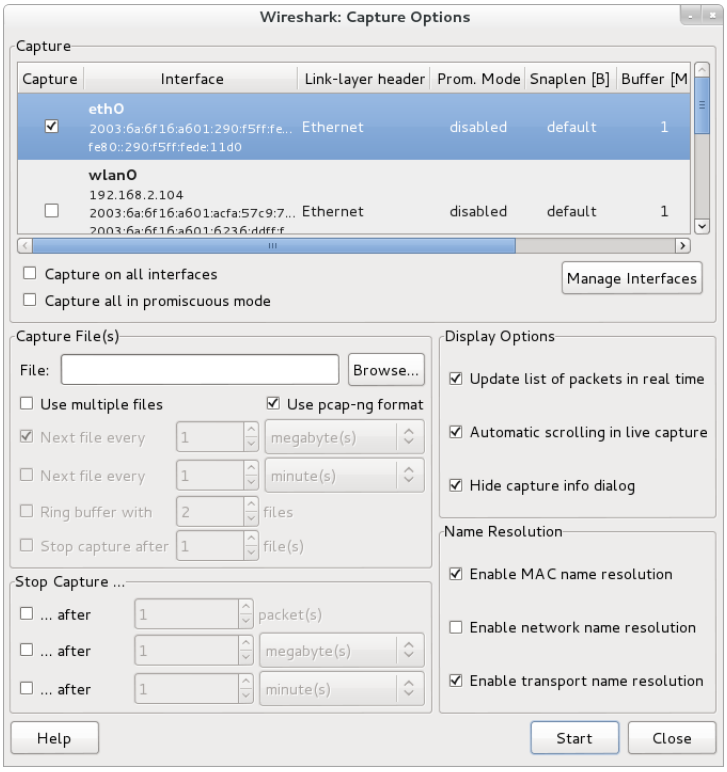
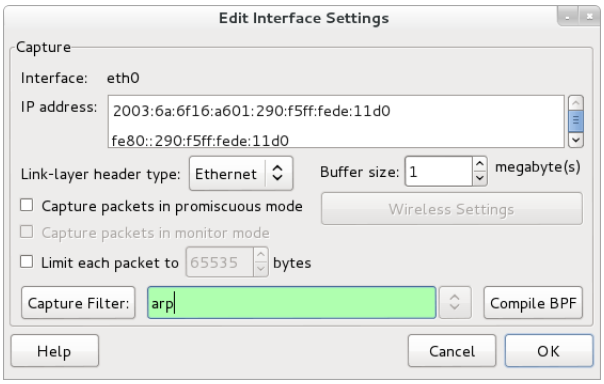
Lösung Wireshark Übung: ARP

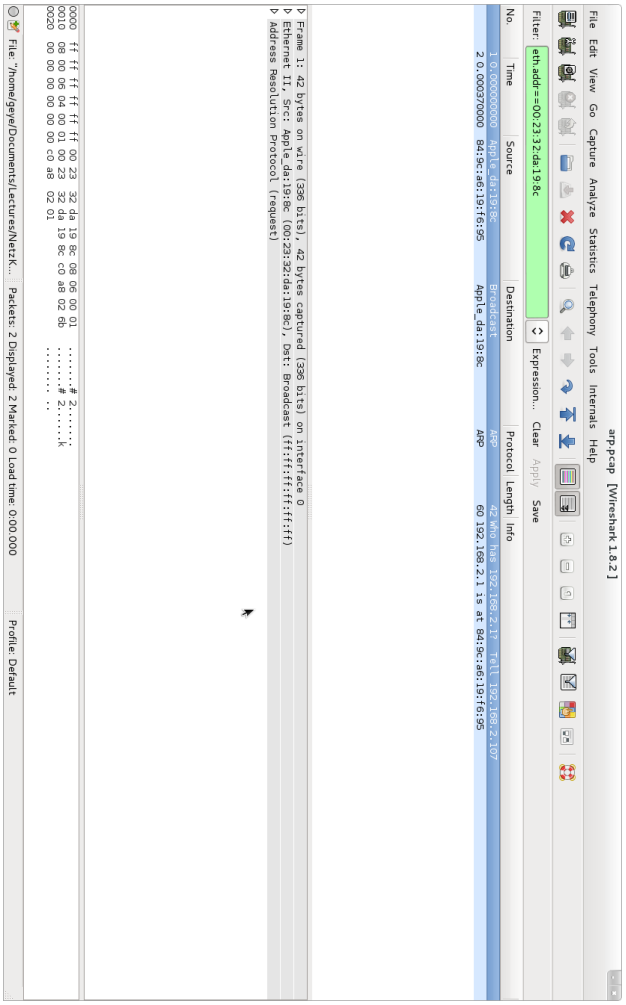
1. Mitschnitt starten, Default Gateway löschen und eine externe Internet-Seite aufrufen:
   (In diesem Dokument beziehen sich alle weiteren Lösungen auf das zur Verfügung gestellte Beispiel Mitschnitt: *"arp.pcap"*





2. Das Löschen des ARP-Caches notwendig um sicher zu gehen, dass ARP Pakete ausgetauscht werden um den ARP Cache neu aufzubauen. Der Aufruf einer externen Internet Seite war notwendig um sicher zu gehen, dass die MAC Adresse (L2 Adressierung) das lokalen Gateway's (default Gateway) per ARP angefragt wird. Das default Gateway wird immer für Anfragen zu externen IP Adressen verwendet und ist Teil der lokalen IP Konfiguration (siehe Befehl „route“ bzw. „Umgebung von ARP“).

3. Display filter um nur Pakete von und zu eigenem Rechner:

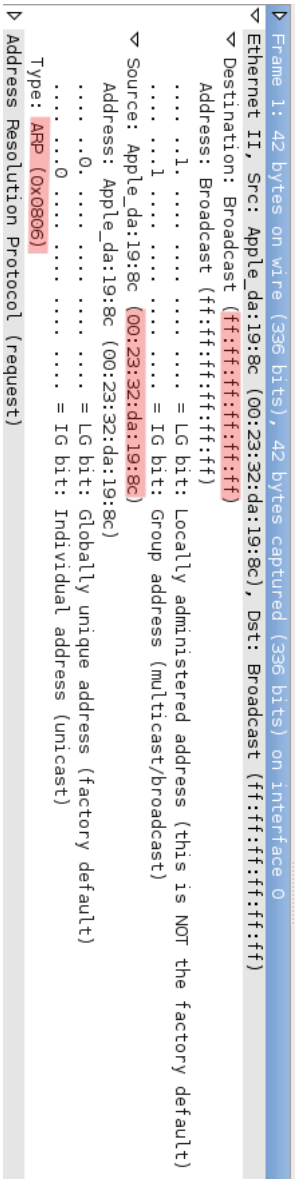


4. ARP Request

(I) Ethernet Block:

a. Quelladresse: $00:23:32:da:19:8c$, (eigene MAC Adresse!)
Zieladresse: $ff:ff:ff:ff:ff:ff$

b. Type: $0x0806$ (ARP)

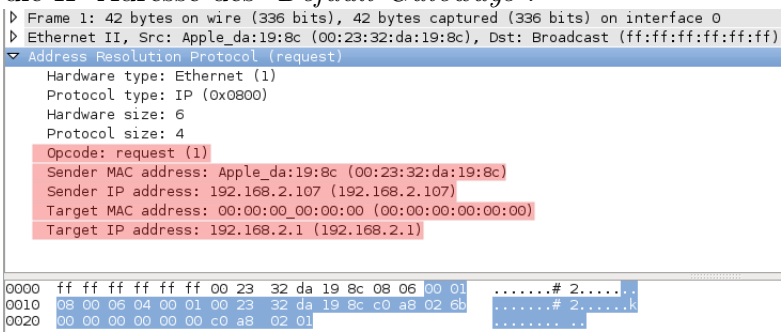


(II) ARP Block:

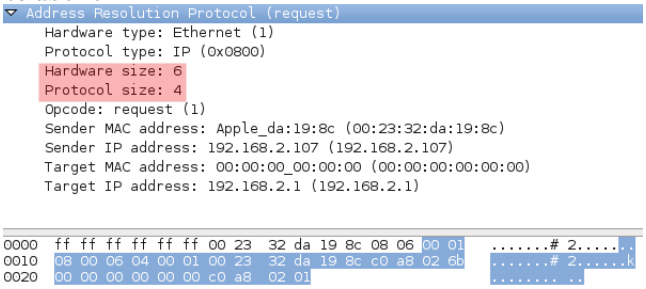
a. Es wird der *"Opcode" 1* verwendet. Dieser zeigt an, dass es sich bei dem ARP Paket um einen *"Request"* handelt.

b. Quelladresse (MAC): $00:23:32:da:19:8c$, IP:192.168.2.107

c. Zieladresse (MAC): $00:00:00:00:00:00 \Rightarrow Null$, diese Adresse wird durch den *"Request"* ermittelt! IP: 192.168.0.1, die IP Adresse des *"Default Gateways"*.



d. Es werden IP (4 Byte) und Mac (6 Byte) Adressen ausgetauscht



5. ARP Reply

   (I) Ethernet Block:

      a. Quelladresse: $84:9c:a6:19:f6:95$, (MAC Adresse des Gateway!)
      Zieladresse: $00:23:32:da:19:8c$ (eigene MAC Adresse)

      b. Type: $0x0806$ (ARP)

   (II) ARP Block:

      a. Es wird der *"Opcode" 2* verwendet. Dieser zeigt an, dass es sich bei dem ARP Paket um einen *"Reply"* handelt.

      b. Quelladresse (MAC): $84:9c:a6:19:f6:95$, hierbei handelt es sich um das nachgefragte Datum! IP: 192.168.0.1, die IP Adresse des *"Default Gateways"*.

      c. Zieladresse (MAC): $00:23:32:da:19:8c$, IP:192.168.2.107

      d. Es werden IP (4 Byte) und Mac (6 Byte) Adressen ausgetauscht