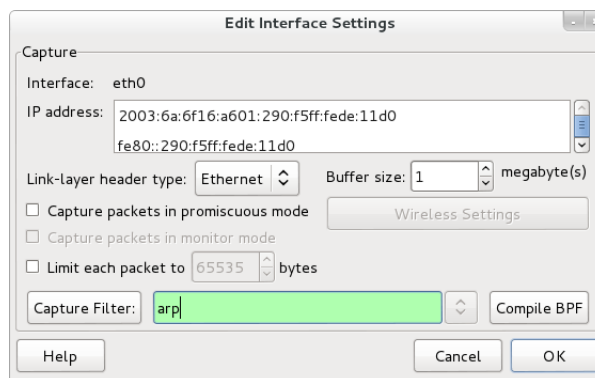
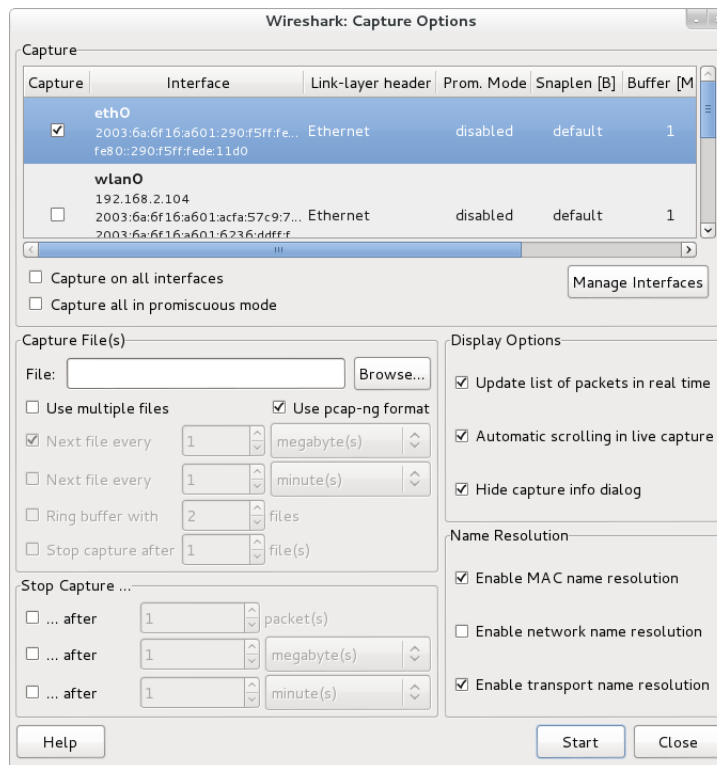


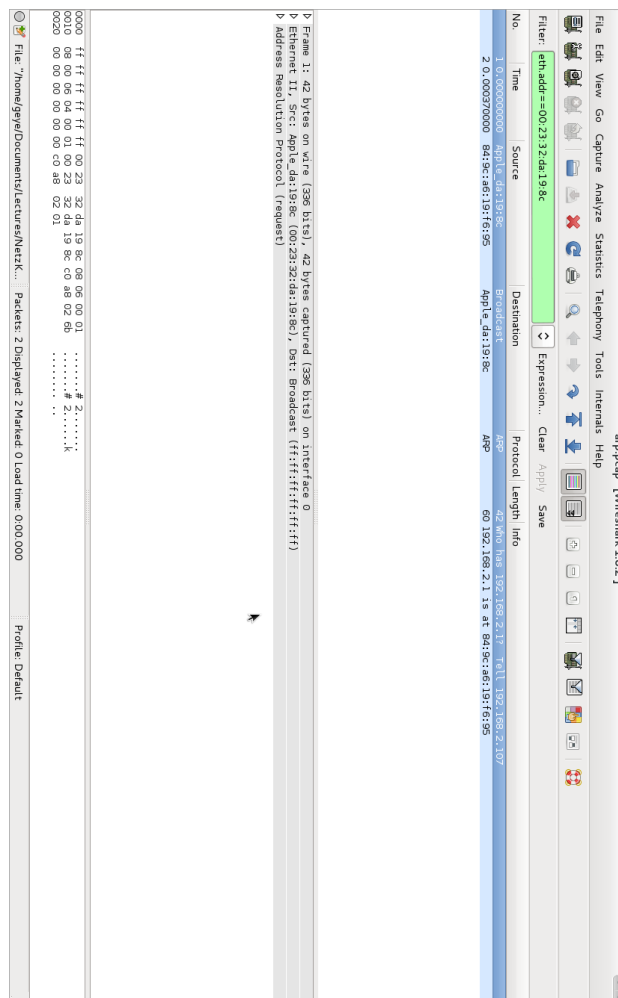
Lösung Wireshark Übung: ARP

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”*)



- 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) des 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“).
- 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)

```

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
  > Ethernet II, Src: Apple_da:19:8c (00:23:32:da:19:8c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
        .....1..... = LG bit: Locally administered address (this is NOT the factory default)
        > Source: Apple_da:19:8c (00:23:32:da:19:8c)
          Address: Apple_da:19:8c (00:23:32:da:19:8c)
            .....0..... = LG bit: Globally unique address (factory default)
            .....0..... = IG bit: Individual address (unicast)
          Type: ARP (0x0806)
    > Address Resolution Protocol (request)
```

(II) ARP Block:

- Es wird der “Opcode” 1 verwendet. Dieser zeigt an, dass es sich bei dem ARP Paket um einen “Request” handelt.
- Quelladresse (MAC): 00 : 23 : 32 : da : 19 : 8c, IP:192.168.2.107
- 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”.

```

▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▶ Ethernet II, Src: Apple_da:19:8c (00:23:32:da:19:8c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Apple_da:19:8c (00:23:32:da:19:8c)
  Sender IP address: 192.168.2.107 (192.168.2.107)
  Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.2.1 (192.168.2.1)

0000  ff ff ff ff ff ff 00 23 32 da 19 8c 08 06 00 01  .....# 2.....
0010  08 00 06 04 00 01 00 23 32 da 19 8c c0 a8 02 6b  .....# 2.....k
0020  00 00 00 00 00 00 c0 a8 02 01  .....

```

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

```

▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Apple_da:19:8c (00:23:32:da:19:8c)
  Sender IP address: 192.168.2.107 (192.168.2.107)
  Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.2.1 (192.168.2.1)

0000  ff ff ff ff ff ff 00 23 32 da 19 8c 08 06 00 01  .....# 2.....
0010  08 00 06 04 00 01 00 23 32 da 19 8c c0 a8 02 6b  .....# 2.....k
0020  00 00 00 00 00 00 c0 a8 02 01  .....

```

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