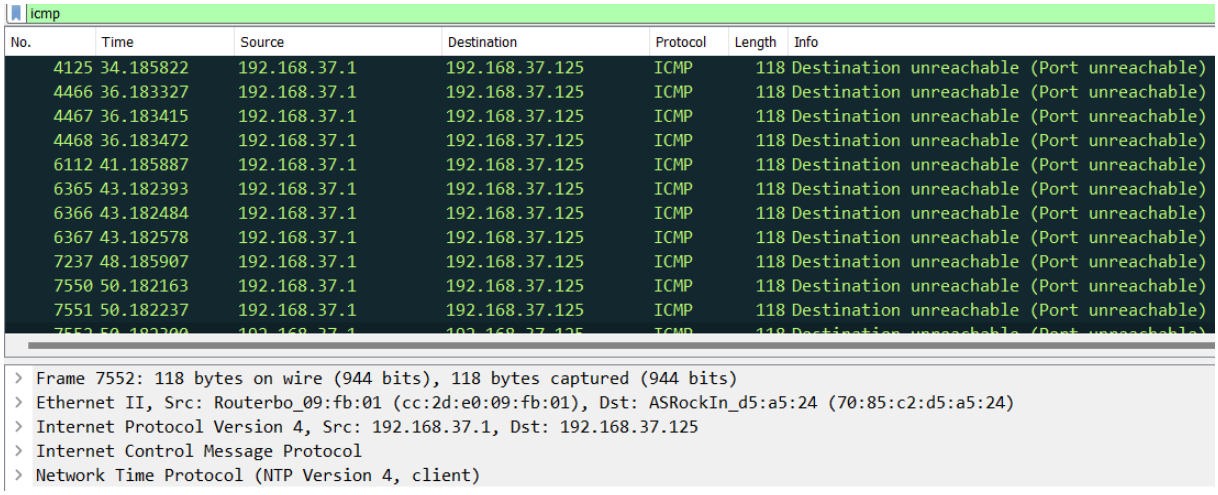
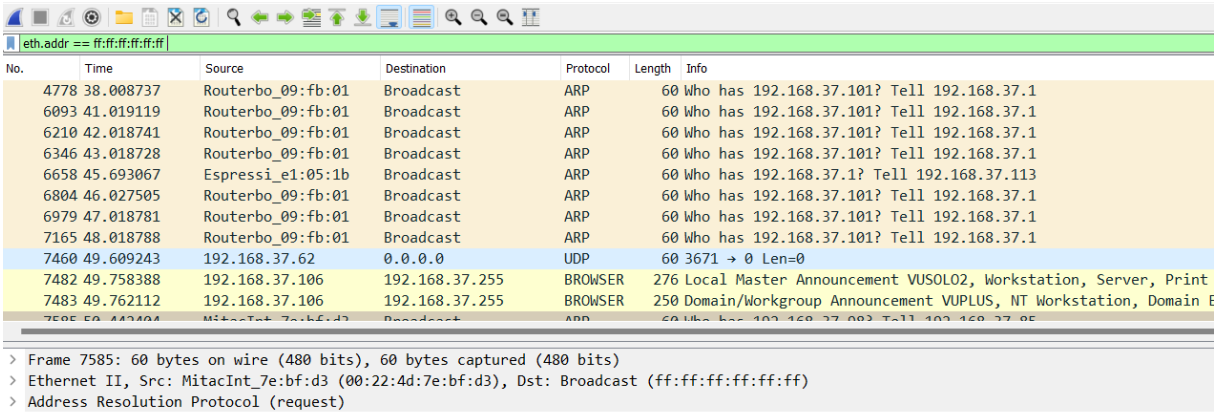
Wireshark Sicherheitsanalyse

Setze geeignete Filter, um folgende Dinge herauszufinden:

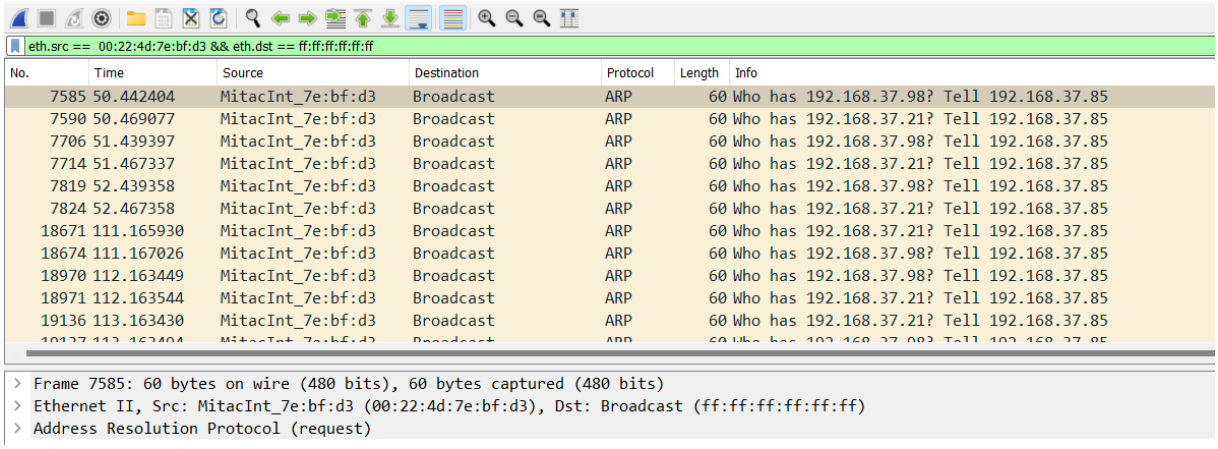
- Wie viele Frames enthalten Daten mit dem Protokoll ICMP?
  Mit dem Filter icmp kann man danach suchen.
  Es sind 179 Frames mit dem Protokoll ICMP



- Wie viele Frames sind ein Ethernet-Broadcast?
  Mit dem Filter eth.addr == ff:ff:ff:ff:ff:ff kann man danach suchen.
  Es sind 103 Frames



- Wie viele Frames sind ein Ethernet-Broadcast von der MAC-Adresse "00:22:4d:7e:bf:d3" gesendet?
  Mit dem Filter eth.src == 00:22:4d:7e:bf:d3 && eth.dst == ff:ff:ff:ff:ff:ff kann man danach suchen
  Es sind 30 Frames



Der Dump enthält auch sicherheitsrelevante Daten wie Benutzernamen und Passwörter.

Finde folgende Frames mittels geeigneter Filter!

- Ein E-Mail wurde unverschlüsselt übertragen. Es enthält als Anhang ein Bild, das eine geheime Nachricht enthält. Wie lautet die geheime Nachricht?
  Mit dem Filter smtp kann man nach E-Mails suchen

```
354 End data with <CR><LF>.<CR><LF>
From: "Michael Fischer" <michael@webfischer.at>
To: "Michael Fischer" <michael.fischer@htlhl.at>
Subject: Streng geheimes Bild
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="MYBOUNDARY"

--MYBOUNDARY
Content-Type: text/plain; charset=utf-8
Content-Disposition: inline

Liebes Ich!

Anbei findest du ein Bild mit der geheimen Botschaft.

Mit freundlichen Gr....en,
Michael Fischer
--MYBOUNDARY
Content-Type: image/png; name="topSecretMessage.png"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="topSecretMessage.png"
```

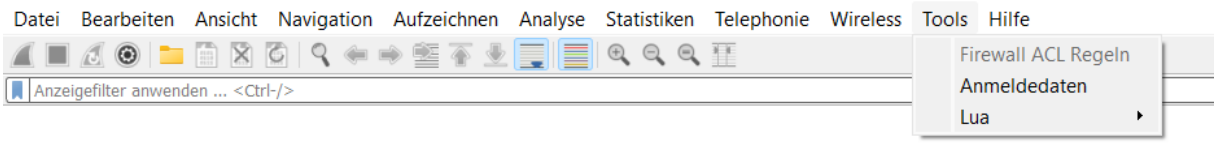
Mit der Seite konnte man Bild decoden: https://codebeautify.org/base64-to-image-converter

Das Bild sieht so aus:

Die geheime Nachricht lautet:
Das ist ein wirklich schönes Platzerl auf fast 3000m

Danach hat ein unverschlüsselter Webseitenaufruf stattgefunden. Die Seite http://mail.webfischer.at/2XHIT wurde aufgerufen. Versuche dich auf der gleichen Webseite einzuloggen und bis zum "final secret" vorzudringen! Wie lautet das "final secret"?

Mit Tools und Anmeldedaten kann man Benutzernamen und Passwörter herausfinden



Das „final secret “lautet: HTLHL rulez!

You are the best!!!
The final secret is: "HTLHL rulez!"

Here, have a potato: