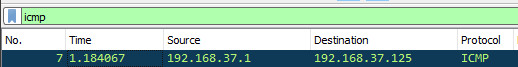
Wireshark Sicherheitsanalyse

# Aufgabe 1:

Wieviele Frames enthalten Daten mit dem Protokoll ICMP?

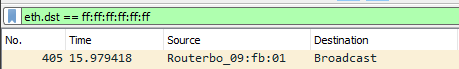
In der Datei „secret.pcap“ sind insgesamt 179 ICMP-Frames enthalten. Dies kann durch die Filterleiste in Wireshark leicht herausgefunden werden.



# Aufgabe 2:

Wieviele Frames sind ein Ethernet-Broadcast?

Dies kann wieder leicht durch die Filterleiste herausgefunden werden. Insgesamt sind 103 Frames Ethernet-Broadcasts.



# Aufgabe 3:

Wieviele Frames sind ein Ethernet-Broadcast von der MAC-Adresse „00:22:4d:7e:bf:d3“

gesendet?

Nochmal kann dies über die Filterleiste gefunden werden. Von der MAC-Adresse sind 30 Frames Broadcasts.

Graphical user interface, text, application, chat or text message  Description automatically generated

# Aufgabe 4:

Ein E-Mail wurde unverschlüsselt übertragen. Es enthält als Anhang ein Bild, das eine geheime Nachricht enthält. Wie lautet die geheime Nachricht?

Die Nachricht kann durch das decoden des base64-Strings zu einer png-Datei gefunden werden. Die geheime Nachricht ist: Das ist ein wirklich schönes Platzerl auf fast 3000m.



**Aufgabe 5:**

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"?

Das erste Passwort kann in einem der http Einträge in Wireshark gefunden werden. Unter dem Punkt „Hypertext Transfer Protokoll“ kann der Punkt „Authorization“ gefunden werden, in diesem kann der Benutzername und das Passwort gefunden werden.



Nach der Eingabe muss noch ein Passwort eingegeben werden. Ein Hinweis zu dem Passwort kann in dem letztem http Eintrag im letzten Punkt gefunden werden.



Ein letztes Passwort ist noch benötigt, dies kann im Quelltext der Seite gefunden werden.

