

# 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

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
4125	34.185822	192.168.37.1	192.168.37.125	ICMP	118	Destination unreachable (Port unreachable)
4466	36.183327	192.168.37.1	192.168.37.125	ICMP	118	Destination unreachable (Port unreachable)
4467	36.183415	192.168.37.1	192.168.37.125	ICMP	118	Destination unreachable (Port unreachable)
4468	36.183472	192.168.37.1	192.168.37.125	ICMP	118	Destination unreachable (Port unreachable)
6112	41.185887	192.168.37.1	192.168.37.125	ICMP	118	Destination unreachable (Port unreachable)
6365	43.182393	192.168.37.1	192.168.37.125	ICMP	118	Destination unreachable (Port unreachable)
6366	43.182484	192.168.37.1	192.168.37.125	ICMP	118	Destination unreachable (Port unreachable)
6367	43.182578	192.168.37.1	192.168.37.125	ICMP	118	Destination unreachable (Port unreachable)
7237	48.185907	192.168.37.1	192.168.37.125	ICMP	118	Destination unreachable (Port unreachable)
7550	50.182163	192.168.37.1	192.168.37.125	ICMP	118	Destination unreachable (Port unreachable)
7551	50.182237	192.168.37.1	192.168.37.125	ICMP	118	Destination unreachable (Port unreachable)
7552	50.182300	192.168.37.1	192.168.37.125	ICMP	118	Destination unreachable (Port unreachable)

> Frame 7552: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)  
 > Ethernet II, Src: Routerbo\_09:fb:01 (cc:2d:e0:09:fb:01), Dst: ASRockIn\_d5:a5:24 (70:85:c2:d5:a5:24)  
 > Internet Protocol Version 4, Src: 192.168.37.1, Dst: 192.168.37.125  
 > Internet Control Message Protocol  
 > Network Time Protocol (NTP Version 4, client)

- ❖ 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

eth.addr == ff:ff:ff:ff:ff:ff						
No.	Time	Source	Destination	Protocol	Length	Info
4778	38.008737	Routerbo_09:fb:01	Broadcast	ARP	60	Who has 192.168.37.101? Tell 192.168.37.1
6093	41.019119	Routerbo_09:fb:01	Broadcast	ARP	60	Who has 192.168.37.101? Tell 192.168.37.1
6210	42.018741	Routerbo_09:fb:01	Broadcast	ARP	60	Who has 192.168.37.101? Tell 192.168.37.1
6346	43.018728	Routerbo_09:fb:01	Broadcast	ARP	60	Who has 192.168.37.101? Tell 192.168.37.1
6658	45.693067	Espressi_e1:05:1b	Broadcast	ARP	60	Who has 192.168.37.1? Tell 192.168.37.113
6804	46.027505	Routerbo_09:fb:01	Broadcast	ARP	60	Who has 192.168.37.101? Tell 192.168.37.1
6979	47.018781	Routerbo_09:fb:01	Broadcast	ARP	60	Who has 192.168.37.101? Tell 192.168.37.1
7165	48.018788	Routerbo_09:fb:01	Broadcast	ARP	60	Who has 192.168.37.101? Tell 192.168.37.1
7460	49.609243	192.168.37.62	0.0.0.0	UDP	60	3671 → 0 Len=0
7482	49.758388	192.168.37.106	192.168.37.255	BROWSER	276	Local Master Announcement VUSOL02, Workstation, Server, Print
7483	49.762112	192.168.37.106	192.168.37.255	BROWSER	250	Domain/Workgroup Announcement VUPLUS, NT Workstation, Domain E
7585	50.442404	MitacInt_7e:bf:d3	Broadcast	ARP	60	Who has 192.168.37.101? Tell 192.168.37.1

> Frame 7585: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)  
 > Ethernet II, Src: MitacInt\_7e:bf:d3 (00:22:4d:7e:bf:d3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 > Address Resolution Protocol (request)

- ❖ 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

No.	Time	Source	Destination	Protocol	Length	Info
7585	50.442404	MitacInt_7e:bf:d3	Broadcast	ARP	60	Who has 192.168.37.98? Tell 192.168.37.85
7590	50.469077	MitacInt_7e:bf:d3	Broadcast	ARP	60	Who has 192.168.37.21? Tell 192.168.37.85
7706	51.439397	MitacInt_7e:bf:d3	Broadcast	ARP	60	Who has 192.168.37.98? Tell 192.168.37.85
7714	51.467337	MitacInt_7e:bf:d3	Broadcast	ARP	60	Who has 192.168.37.21? Tell 192.168.37.85
7819	52.439358	MitacInt_7e:bf:d3	Broadcast	ARP	60	Who has 192.168.37.98? Tell 192.168.37.85
7824	52.467358	MitacInt_7e:bf:d3	Broadcast	ARP	60	Who has 192.168.37.21? Tell 192.168.37.85
18671	111.165930	MitacInt_7e:bf:d3	Broadcast	ARP	60	Who has 192.168.37.21? Tell 192.168.37.85
18674	111.167026	MitacInt_7e:bf:d3	Broadcast	ARP	60	Who has 192.168.37.98? Tell 192.168.37.85
18970	112.163449	MitacInt_7e:bf:d3	Broadcast	ARP	60	Who has 192.168.37.98? Tell 192.168.37.85
18971	112.163544	MitacInt_7e:bf:d3	Broadcast	ARP	60	Who has 192.168.37.21? Tell 192.168.37.85
19136	113.163430	MitacInt_7e:bf:d3	Broadcast	ARP	60	Who has 192.168.37.21? Tell 192.168.37.85
19137	113.163404	MitacInt_7e:bf:d3	Broadcast	ARP	60	Who has 192.168.37.98? Tell 192.168.37.85

> Frame 7585: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)  
 > Ethernet II, Src: MitacInt\_7e:bf:d3 (00:22:4d:7e:bf:d3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 > Address Resolution Protocol (request)

## 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 `smtip` 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:**

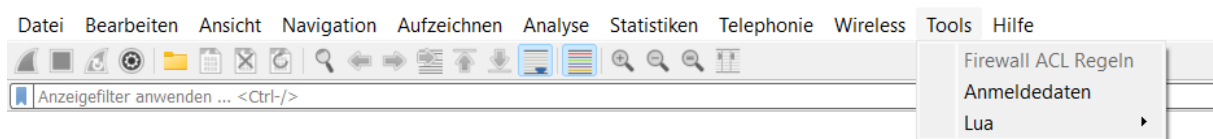


**Die geheime Nachricht lautet:**

**Das ist ein wirklich schönes Platzl 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:

