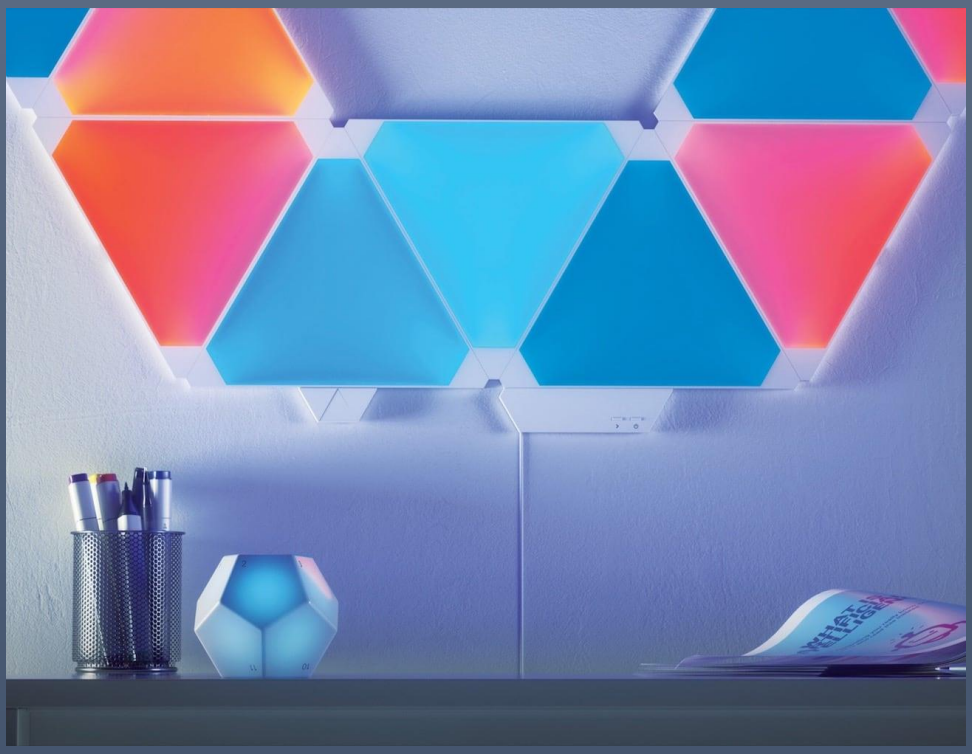
2019



Wahlfachprojekt

DISRUPTING NANOLEAF LIGHT PANELS

Inhaltsverzeichnis

1. Hardware

Nanoleaf Light Panels

Firmware 2.3.0
Hardware Version: 1.6.2
MAC Adresse: 00:55:DA:52:88:1B
IP-Adresse: 192.168.0.129

1.1. Amazon Alexa

Firmware: 618571520
MAC Adresse: 38:F7:3D:2E:98:FC
IP-Adresse: 192.168.0.127

2. Zielsetzung

Ziel dieses Projekts ist es die Funktion von Amazon Alexa in Kombination mit Nanoleaf zu stören. Dabei wird eine Man-in-the-Middle Attacke durchgeführt und somit die gewünschte Information gewonnen und anschließend blockiert.

3. nmap

Als erstes wurde versucht mittels nmap offene Ports zu erkennen. Der nmap Scan wurde sowohl auf die IP-Adresse von Amazon Alexa als auch auf den Nanoleaf Light Panels durchgeführt.

Abbildung 1: Topologie

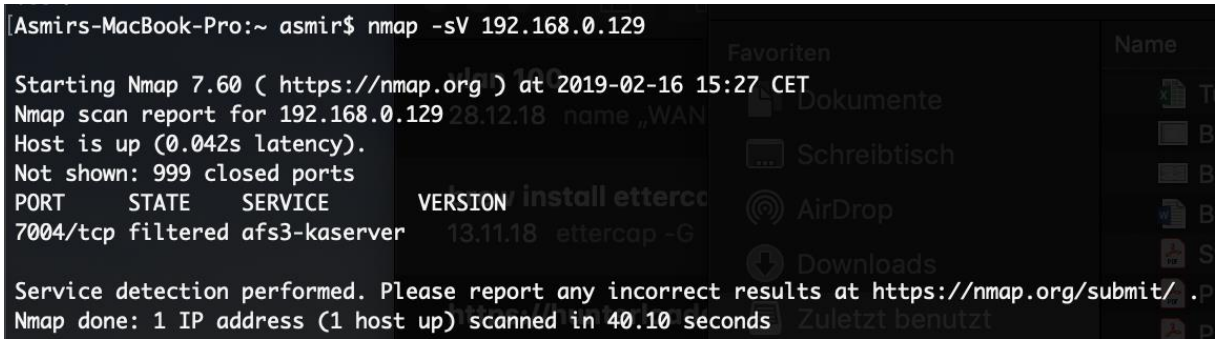
3.1. nmap Alexa

Mittels nmap konnten keine offenen Ports erkannt werden.

```
[Asmirs-MacBook-Pro:~ asmir$ nmap -sV 192.168.0.227

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-13 20:07 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.29 seconds
[Asmirs-MacBook-Pro:~ asmir$ nmap -Pn 192.168.0.227

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-13 20:07 CET
Nmap scan report for 192.168.0.227
Host is up (0.055s latency).
All 1000 scanned ports on 192.168.0.227 are filtered (960) or closed (40)

Nmap done: 1 IP address (1 host up) scanned in 11.31 seconds
Asmirs-MacBook-Pro:~ asmir$
```

3.2. nmap Nanoleaf Light Panels

Mittels nmap konnten keine offenen Ports erkannt werden, welcher für einen Angriff genutzt werden kann. Port 7004 mit dem AFS Kerberos authentication service wurde erkannt, kann jedoch nicht für Angriffe verwendet werden.



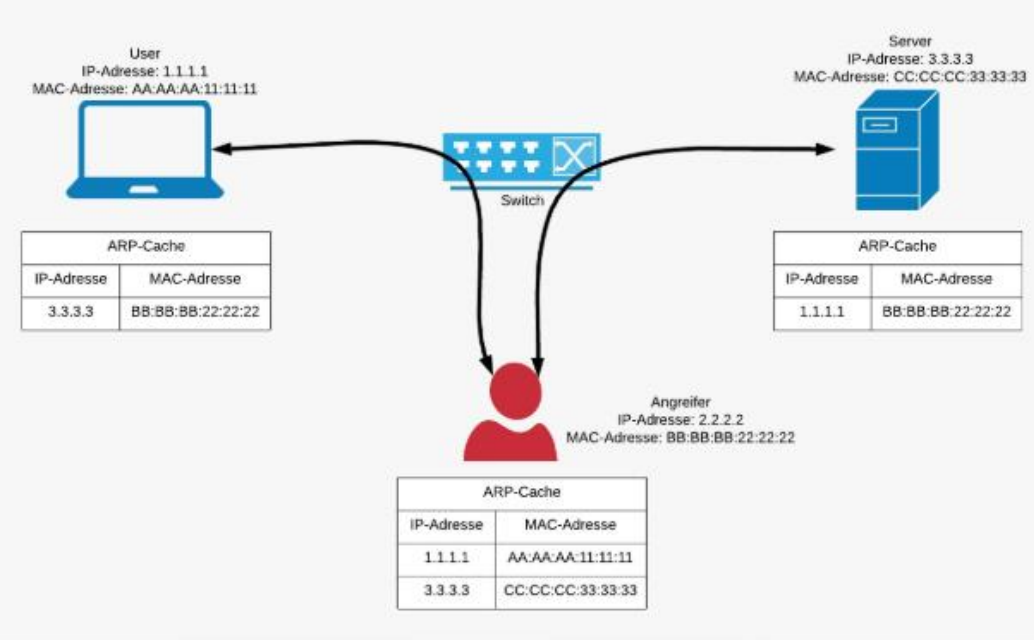
4. ARP Spoofing

4.1. Definition

In Computernetzwerken ist ARP-Spoofing, ARP-Cache-Vergiftung oder ARP-Gift-Routing eine Technik, mit der ein Angreifer Nachrichten des Address Resolution Protocol (ARP) an ein lokales Netzwerk sendet. Im Allgemeinen besteht das Ziel darin, die MAC-Adresse des Angreifers mit der IP-Adresse eines anderen Hosts, wie beispielsweise des Standard-Gateways, zu verknüpfen, so dass jeglicher Datenverkehr darüber umgeleitet wird.

ARP-Spoofing kann es einem Angreifer ermöglichen, Datenpakete in einem Netzwerk abzufangen, den Datenverkehr zu ändern oder den gesamten Datenverkehr zu stoppen. Häufig wird der Angriff als Öffnung für andere Angriffe genutzt, wie z.B. Denial of Service, Man in the Middle oder Session Hijacking Angriffe.

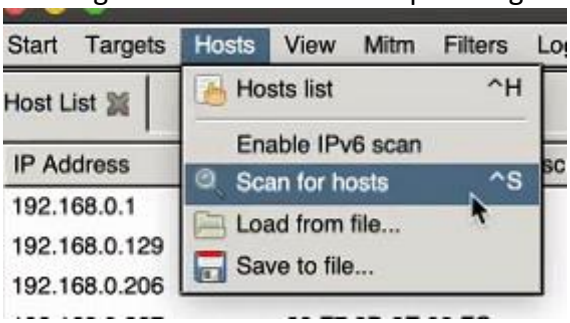
Der Angriff kann nur in Netzwerken, welche ARP verwenden, verwendet werden und erfordert, dass der Angreifer direkten Zugriff auf das anzugreifende lokale Netzwerksegment hat.



Quelle: Eigene Darstellung.

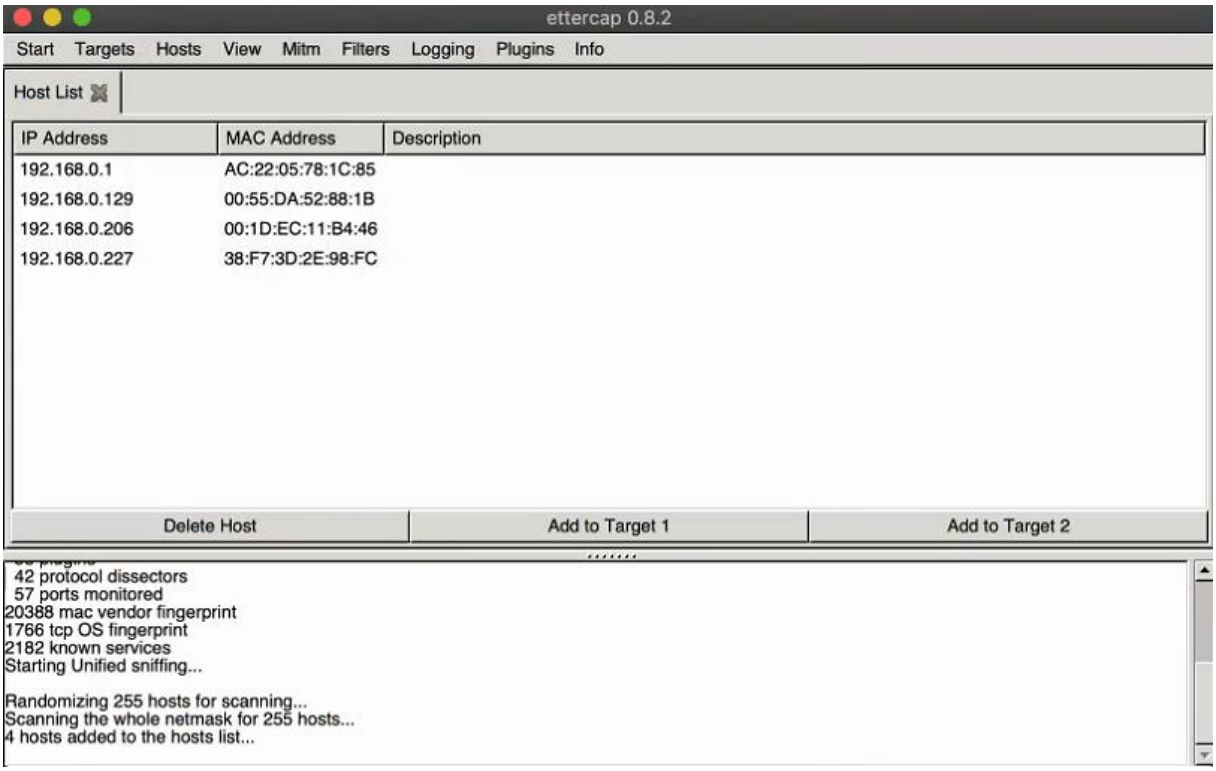
4.2. Ettercap

Der Angriff wird mittels Ettercap durchgeführt.



Nachdem die Anwendung gestartet wurde, wird ein Hostscan in dem Netzwerk durchgeführt. Dadurch werden alle verbundenen Geräte im Netzwerk mit deren MAC Adresse und IP-Adresse dargestellt. Dies ist auf dem folgenden Screenshot ersichtlich.

Die IP-Adresse und MAC Adresse von Amazon Alexa (192.168.0.127) und der Nanoleaf Light Panels werden korrekt angezeigt.

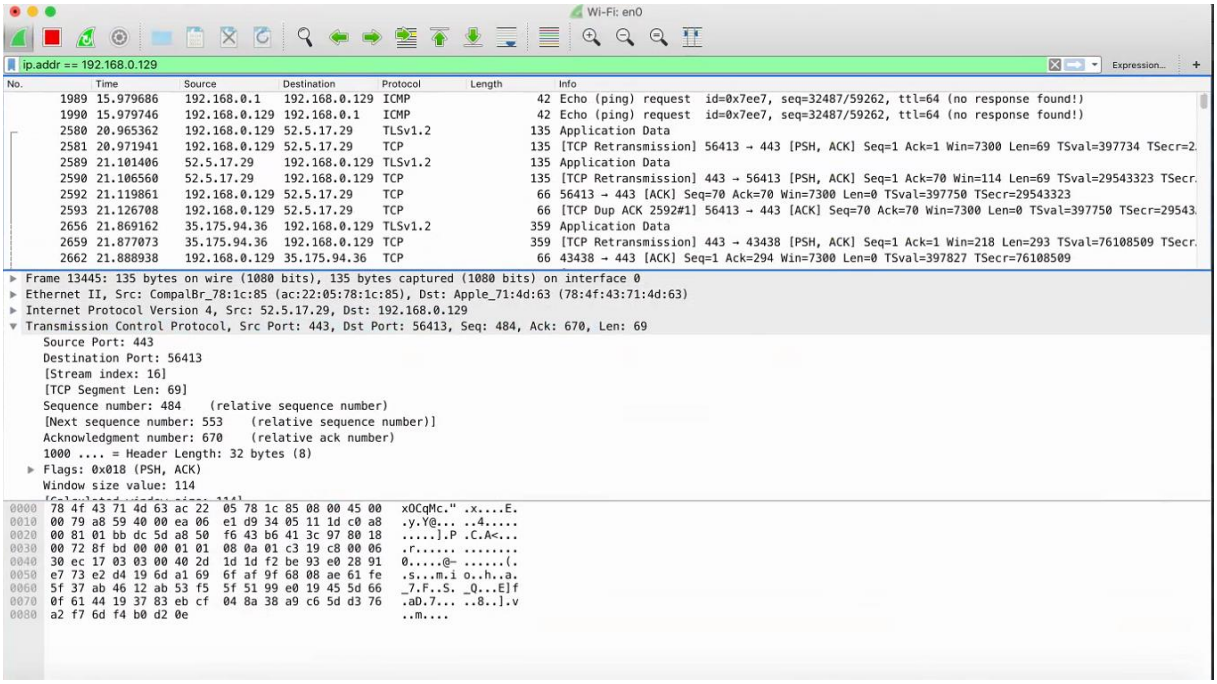


Im nächsten Schritt wurde das Target ausgewählt. Hierbei wurde die IP-Adresse von den Nanoleaf Light Panels als Target 1 ausgewählt und die IP-Adresse des Routers als Target 2 definiert.

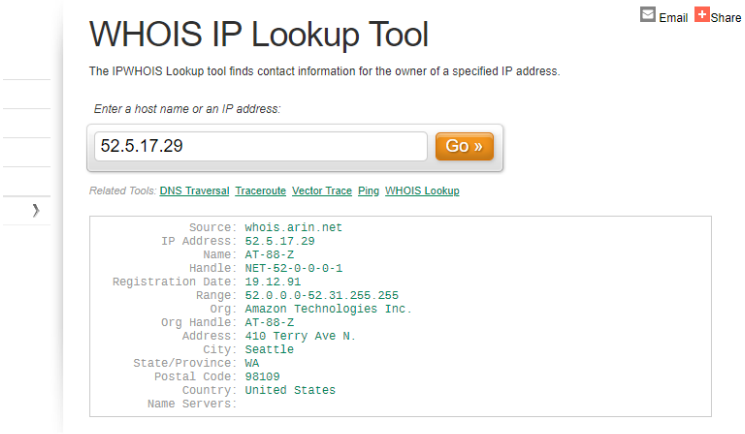
Nachdem dies durchgeführt wurde, wurde der MITM Angriff mittel ARP Poisoning gestartet.

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
7 hosts added to the hosts list...
Host 192.168.0.129 added to TARGET1
Host 192.168.0.1 added to TARGET2
```

Dabei werden beide Richtungen der Kommunikation mitgeschnitten.



Wie im Trace ersichtlich, kommuniziert Nanoleaf direkt mit den Servern von Amazon.
Die beiden IP-Adressen (52.5.17.29) sind auf Amazon registriert (WHOIS IP Abfrage).



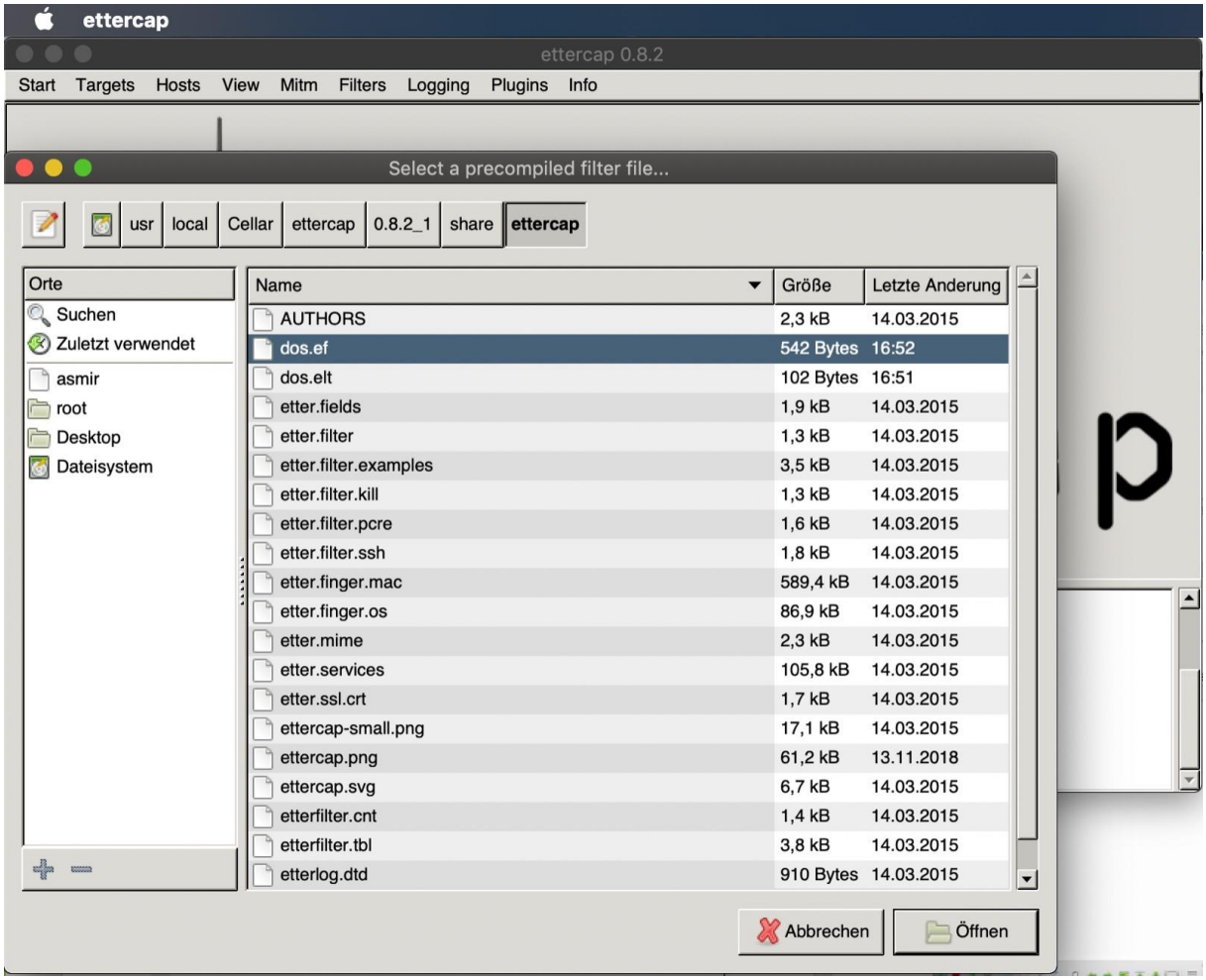
Anschließend wurde mittels Ettercap ein Filter definiert, um die Kommunikation zu stören und somit die Funktionalität der Nanoleaf Light Panels zu beeinträchtigen.
Dazu wurde unter /usr/local/share/ettercap die Datei dos.elt mit folgendem Inhalt erzeugt.

```
if (ip.src == '192.168.0.129' || ip.dst == '52.5.17.29')
{
drop();
kill();
msg("Packet Dropped\n");
}
```

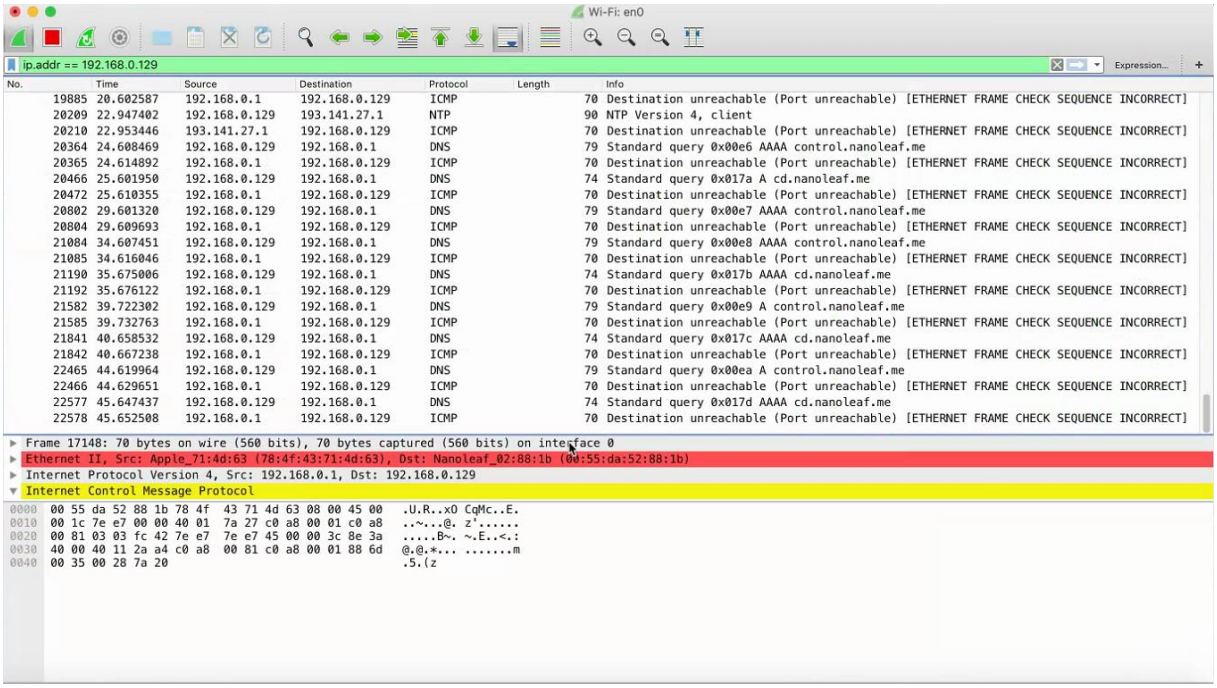
Damit der Filter verwendet werden kann, muss dieser zuerst kompiliert werden.

```
etterfilter dos.elt -o dos.ef
```

Um den Filter anzuwenden, wurde dieser über Ettercap -> Filters -> Select precompiled Filter ausgewählt und somit aktiviert.



In dem darauffolgenden Wiresharek Trace lässt sich erkennen, dass die Nanoleaf Light Panels nicht mehr in der Lage sind die Kommunikation zu den Servern von Amazon herzustellen. In folge dessen, ist die Funktionalität des Nanoleafs gestört und das Ziel dieses Projektes somit erreicht.



Nachdem der Filter wieder deaktiviert wurde, funktionierte das Ändern der Farbe mittels Amazon Alexa wieder wie gewohnt.